LEHRBUCH

DER

ALGEBRA

VON

HEINRICH WEBER

PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT STRASSBURG

ZWEITE AUFLAGE

DRITTER BAND

MIT ZWEI ABBILDUNGEN IM TEXT

BRAUNSCHWEIG

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN

1908

ELLIPTISCHE
FUNKTIONEN
UND
ALGEBRAISCHE ZAHLEN

VON

HEINRICH WEBER

PROFESSOR DER MATHEMATIK AN DER UNIVERSITÄT STRASSBURG

ZWEITE AUFLAGE

MIT ZWEI ABBILDUNGEN IM TEXT

BRAUNSCHWEIG

DRUCK UND VERLAG VON FRIEDRICH VIEWEG UND SOHN

1908

Published May 24, 1908.
Privilege of Copyright in the United States reserved under the Act approved March 3, 1905 by Friedr. Vieweg & Sohn, Braunschweig, Germany.

RICHARD DEDEKIND,

DAVID HILBERT, HERMANN MINKOWSKI

IN HERZLICHER FREUNDSCHAFT

GEWIDMET.

VORWORT.

Es ist mir vergönnt, den Plan einer Weiterführung meines Lehrbuches der Algebra, den ich vor zwölf Jahren in der Vorrede zur ersten Auflage des zweiten Bandes angekündigt habe, nach mannigfaltigen Abhaltungen noch auszuführen. Durch das Entgegenkommen der Verlagsfirma erscheint dieser dritte Band der Algebra zugleich als zweite Auflage der im Jahre 1891 zum erstenmal gedruckten „Elliptischen Funktionen und algebraischen Zahlen".

Er beschäftigt sich hauptsächlich mit dem weiteren Ausbau der mannigfaltigen Anwendungen der Algebra und besonders der Theorie der quadratischen Körper auf die aus den elliptischen Funktionen hervorgegangenen Probleme, die uns das erste über die Kreisteilung hinausgehende Beispiel von algebraischen Zahlen liefern, deren Gesetze einigermaßen bekannt sind. Als Grundlage dazu dient eine eingehendere Behandlung der quadratischen Körper mit negativer Diskriminante. Freilich ist auch hier nicht alles erreicht, was ich mir als letztes Ziel gesteckt hatte. So mußte die Ausführung der Theorie der relativ zyklischen Körper noch zurückgestellt werden — hoffentlich nur einstweilen.

Dagegen habe ich, einem mehrfach an mich herangetretenen Wunsche entsprechend, einen Abriß der Theorie der algebraischen Funktionen auf arithmetischer Grundlage beigefügt, der

sich im wesentlichen an die Abhandlung von Dedekind und mir im 92. Bande von Crelles Journal anschließt, aber durch Anwendung der Theorie der Funktionale, auf die ich im zweiten Bande die Theorie der algebraischen Zahlen gegründet habe, wie mir scheint, eine Vereinfachung erreicht.

Straßburg, im Mai 1908.

H. Weber.

INHALTSVERZEICHNIS.

Erstes Buch.

Analytischer Teil.

Erster Abschnitt.

Die elliptischen Integrale.

Zweiter Abschnitt.

Theta-Funktionen.

Dritter Abschnitt.

Transformation der Theta-Funktionen.

Vierter Abschnitt.

Die elliptischen Funktionen.

Fünfter Abschnitt.

Die Modulfunktionen.

Sechster Abschnitt.

Multiplikation und Teilung der elliptischen Funktionen.

Siebenter Abschnitt.

Theorie der Transformationsgleichungen.

Achter Abschnitt.

Die Gruppe der Transformationsgleichungen und die Gleichung 5ten Grades.

Zweites Buch.

Quadratische Körper.

Neunter Abschnitt.

Diskriminante.

Zehnter Abschnitt.

Algebraische Zahlen und Formen.

Elfter Abschnitt.

Ideale in quadratischen Körpern.

Zwölfter Abschnitt.

Ordnungen im quadratischen Körper.

Dreizehnter Abschnitt.

Äquivalenz nach Zahlgruppen.

Vierzehnter Abschnitt.

Komposition der Formen und Ideale.

Fünfzehnter Abschnitt.

Geschlechter der quadratischen Formen.

Sechzehnter Abschnitt.

Klassenzahl in quadratischen Körpern.

Drittes Buch.

Komplexe Multiplikation.

Siebzehnter Abschnitt.

Elliptische Funktionen und quadratische Formen.

Achtzehnter Abschnitt.

Galoissche Gruppe der Klassengleichung.

Neunzehnter Abschnitt.

Berechnung der Klasseninvarianten.

Zwanzigster Abschnitt.

Die Multiplikatorgleichung in der komplexen Multiplikation.

Einundzwanzigster Abschnitt.

Die Normen der Klasseninvarianten $f(\omega)$.

Zweiundzwanzigster Abschnitt.

Cayleys Entwickelung der Modulfunktionen.

Viertes Buch.

Klassenkörper.

Dreiundzwanzigser Abschnitt.

Der Teilungskörper.

Fünftes Buch.

Algebraische Funktionen.

Vierundzwanzigster Abschnitt.

Algebraische Funktionen einer Variablen.

Fünfundzwanzigster Abschnitt.

Funktionale.

Sechsundzwanzigster Abschnitt.

Zahlenwerte der algebraischen Funktionen.

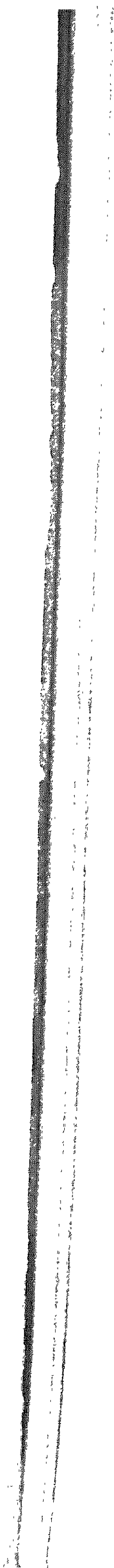
Siebenundzwanzigster Abschnitt.

Algebraische und Abelsche Differentiale.

Tabellen.

ERSTES BUCH.

ANALYTISCHER TEIL.



Erster Abschnitt.

Die elliptischen Integrale.

§ 1. Definition der elliptischen Integrale.

Wenn die systematische Darstellung der Integralrechnung bis zu dem Punkte gelangt ist, wo algebraische Integrale mit der Quadratwurzel aus einer Funktion ersten oder zweiten Grades auf Integrale rationaler Funktionen zurückgeführt werden, so tritt an dieser Stelle dem Lernenden eine Schranke entgegen, die er mit den ihm bis dahin zu Gebote stehenden Hilfsmitteln nicht zu übersteigen imstande ist. Das Streben nach einer Erweiterung der Hilfsmittel, um auch noch die nächste Klasse von Integralen der Forschung zugänglich zu machen, ist, wie es historisch der Anlaß gewesen, zu einem eingehenderen Studium der elliptischen Integrale und zur Einführung der elliptischen Funktionen, auch der naturgemäßeste und verständlichste Ausgangspunkt für den, der in die Theorie dieser Funktionen zuerst eingeführt werden soll. Es soll daher auch unsere nächste Aufgabe sein, uns mit den elliptischen Integralen und ihren wichtigsten Eigenschaften bekannt zu machen.

Die Definition eines elliptischen Integrals, von der wir ausgehen wollen, ist die folgende: Es bedeute $f(x)$ eine ganze rationale Funktion dritten oder vierten Grades mit vier verschiedenen Wurzeln

$$(1) \qquad f(x) = a_0 x^4 + 4 a_1 x^3 + 6 a_2 x^2 + 4 a_3 x + a_4,$$

worin a_0 und a_1 nicht beide zugleich verschwinden; es sei ferner $\Phi(x, y)$ eine beliebige ganze oder gebrochene rationale Funktion der beiden Argumente x, y. Dann ist

$$\int \Phi(x, \sqrt{f(x)})\, dx$$

das allgemeine elliptische Integral und

$$\Phi(x, \sqrt{f(x)})\, dx$$

und nennen dies eine lineare Substitution. Deuten wir x und x' wie im § 1 als Punkte auf zwei geraden Linien L und L', so ist durch (2) eine gegenseitig eindeutige Beziehung der Punkte von L und L', eine Abbildung, festgelegt. Den Werten $x = \infty$ und $x' = \infty$ entsprechen die unendlich fernen Teile der Geraden, die wir ebenfalls als bestimmte Punkte betrachten. Es entspricht dann der Punkt $x' = \infty$ dem Punkt $x = \alpha : \gamma$ und der Punkt $x = \infty$ dem Punkt $x' = -\delta : \gamma$, und nur wenn $\gamma = 0$, die Substitution (2) also ganz ist, entsprechen sich die unendlich fernen Punkte auf L und L' gegenseitig.

Die Substitution (2) ändert sich nicht, wenn die vier Transformationszahlen mit demselben Faktor multipliziert werden. Die Determinante r vervielfältigt sich mit dem Quadrate dieses Faktors, und man kann daher diesen Faktor so bestimmen, daß die Determinante einen beliebig gegebenen Wert, z. B. den Wert 1 erhält.

Wendet man die Substitution (2) auf irgend zwei Punkte x_1, x_2 und die zugehörigen x_1', x_2' an, so ergibt sich

$$(x_1 x_2) = \frac{r(x_1' x_2')}{(\gamma x_1' + \delta)(\gamma x_2' + \delta)},$$

und wenn man ein zweites Punktepaar x_3, x_4 und das entsprechende x_3', x_4' hinzunimmt:

$$(x_1 x_2)(x_3 x_4) = \frac{r^2 (x_1' x_2')(x_3' x_4')}{(\gamma x_1' + \delta)(\gamma x_2' + \delta)(\gamma x_3' + \delta)(\gamma x_4' + \delta)}.$$

Vertauscht man hierin x_2 mit x_3 und bildet den Quotienten, so folgt

$$(3) \qquad \frac{(x_1 x_2)(x_3 x_4)}{(x_1 x_3)(x_2 x_4)} = \frac{(x_1' x_2')(x_3' x_4')}{(x_1' x_3')(x_2' x_4')}.$$

Der Ausdruck auf der linken Seite wird das Doppelverhältnis des Punktepaares $x_1 x_4$ zu dem Punktepaar $x_2 x_3$ genannt, und es ist also in dieser Formel der Satz enthalten:

Das Doppelverhältnis zweier Punktepaare ist bei gleichzeitiger linearer Transformation der vier Punkte invariant.

Vier Punkte lassen sich auf sechs Arten in zwei Paare zerlegen. Setzen wir aber

$$\begin{aligned} a &= (x_2 x_3)(x_1 x_4) \\ b &= (x_3 x_1)(x_2 x_4), \\ c &= (x_1 x_2)(x_3 x_4) \end{aligned}$$

so besteht die Identität:

$$(4) \qquad a + b + c = 0$$

und wir erhalten die sechs Doppelverhältnisse

$$(5) \qquad \begin{matrix} -\frac{c}{b}, & -\frac{a}{c}, & -\frac{b}{a}, \\ -\frac{b}{c}, & -\frac{c}{a}, & -\frac{a}{b}; \end{matrix}$$

setzen wir das erste von ihnen $-c:b = \varkappa^2$, so erhält man nach (4) die sechs:

$$(6) \qquad \varkappa^2, \quad \frac{\varkappa^2-1}{\varkappa^2}, \quad \frac{1}{1-\varkappa^2}, \quad \frac{1}{\varkappa^2}, \quad \frac{\varkappa^2}{\varkappa^2-1}, \quad 1-\varkappa^2.$$

Es sind also die sechs Doppelverhältnisse aus den vier Punkten linear durch eines unter ihnen ausgedrückt.

Wenn die x_1, x_2, x_3, x_4 untereinander permutiert werden, so werden die a, b, c untereinander permutiert und ändern ihre Vorzeichen, jedoch so, daß entweder alle drei Vorzeichen gleichzeitig geändert werden oder ungeändert bleiben. Beispielsweise geben die Transpositionen

$$(14) \text{ und } (23) \qquad \begin{pmatrix} a & b & c \\ -a & -c & -b \end{pmatrix}$$

$$(24) \text{ und } (31) \qquad \begin{pmatrix} a & b & c \\ -c & -b & -a \end{pmatrix}$$

$$(34) \text{ und } (12) \qquad \begin{pmatrix} a & b & c \\ -b & -a & -c \end{pmatrix}$$

Wenn x_1, x_2, x_3, x_4, reell sind, so wird $\varkappa^2$ dann und nur dann ein positiver echter Bruch, wenn $\varkappa^2$ und $1 - \varkappa^2$ positiv, also entweder a und c positiv und b negativ oder a und c negativ, b positiv ist. Dies findet statt, wenn x_1, x_2, x_3, x_4 in dieser Reihenfolge der Größe nach aufsteigend einander folgen und bei allen den Anordnungen, die daraus durch solche Permutationen entstehen, die b ungeändert lassen. Dies sind die folgenden acht:

1	2	3	4
2	3	4	1
3	4	1	2
4	1	2	3
1	4	3	2
4	3	2	1
3	2	1	4
2	1	4	3

Denkt man sich also x_1, x_2, x_3, x_4 in dieser Reihenfolge auf eine Kreisperipherie gesetzt, so erhält man immer dann ein positives echt gebrochenes $\varkappa^2$, wenn die x_i so der Größe nach aufeinander folgen, daß man mit einem beliebigen als kleinstem anfängt und dann auf dem Kreise entweder nach rechts oder nach links weiter zählt. Wir drücken dies so aus:

Damit $\varkappa^2$ ein positiver echter Bruch sei, müssen die Größen x_1, x_2, x_3, x_4 der Größe nach zyklisch aufeinander folgen.

§ 3. Lineare Transformation des elliptischen Differentials.

Wenn sich die beiden Punkte x_3 und x_4 einem und demselben Punkte x annähern, so nähern sich x'_3 und x'_4 dem entsprechenden Punkte x' an. Wir setzen dann $(x_3 x_4):(x'_3 x'_4) = dx:dx'$ und erhalten aus (3), § 2, die Beziehung zwischen den Differentialen dx, dx':

$$(1)\qquad \frac{(x_1 x_2)\,dx}{(x_1 x)(x_2 x)} = \frac{(x'_1 x'_2)\,dx'}{(x'_1 x')(x'_2 x')}.$$

Ebenso ergibt sich, wenn man an Stelle von x_1, x_2 zwei andere Punkte x_3, x_4 setzt:

$$(2)\qquad \frac{(x_3 x_4)\,dx}{(x_3 x)(x_4 x)} = \frac{(x'_3 x'_4)\,dx'}{(x'_3 x')(x'_4 x')},$$

und wenn man multipliziert und die Wurzel zieht:

$$(3)\qquad \frac{\sqrt{(x_1 x_2)(x_3 x_4)}\,dx}{\sqrt{(x_1 x)(x_2 x)(x_3 x)(x_4 x)}} = \frac{\sqrt{(x'_1 x'_2)(x'_3 x'_4)}\,dx'}{\sqrt{(x'_1 x')(x'_2 x')(x'_3 x')(x'_4 x')}},$$

also eine Transformation des elliptischen Differentials durch eine lineare Substitution:

$$x = \frac{\alpha x' + \beta}{\gamma x' + \delta}.$$

Diese Substitution ist vollkommen bestimmt, wenn zu drei beliebigen Punkten x_1, x_2, x_3 die zugehörigen Werte x'_1, x'_2, x'_3 willkürlich gegeben sind, und man erhält sie aus der Gleichheit des Doppelverhältnisses:

$$(4)\qquad \frac{(x_1 x_2)(x_3 x)}{(x_1 x_3)(x_2 x)} = \frac{(x'_1 x'_2)(x'_3 x')}{(x'_1 x'_3)(x'_2 x')},$$

durch Auflösung nach x, und den vierten zu x_4 gehörigen Wert x'_4 erhält man aus

(5) $$\frac{(x_1 x_2)(x_3 x_4)}{(x_1 x_3)(x_2 x_4)} = \frac{(x_1' x_2')(x_3' x_4')}{(x_1' x_3')(x_2' x_4')}.$$

Wenn die Funktion $f(x)$ in dem elliptischen Differential

$$du = \frac{dx}{\sqrt{f(x)}}$$

gegeben ist, so sind damit auch die x_1, x_2, x_3, x_4 gegeben, und durch die lineare Transformation (3) kann man das Differential auf eine andere Form bringen, bei der drei der Größe x_1', x_2', x_3', x_4' beliebig gegebene Werte haben. Man erhält die Normalform, wenn man

$$x' = z, \quad x_1' = 0, \quad x_2' = 1, \quad x_3' = \frac{1}{\varkappa^2}, \quad x_4' = \infty$$

annimmt. Die Größe $\varkappa$ heißt bei Legendre der Modul des elliptischen Differentials und $\sqrt{1 - \varkappa^2} = \varkappa'$ das Komplement des Moduls. Ordnet man also die Punkte in folgender Weise einander zu:

$$\begin{array}{ccccc} z, & 0, & 1, & \frac{1}{\varkappa^2}, & \infty, \\ x, & x_1, & x_2, & x_3, & x_4, \end{array}$$

so ergeben sich aus der Gleichheit der Doppelverhältnisse leicht die Relationen:

(6) $$\begin{aligned} z &= \frac{(x x_1)(x_2 x_4)}{(x x_4)(x_2 x_1)}, \\ 1 - z &= \frac{(x x_2)(x_1 x_4)}{(x x_4)(x_1 x_2)}, \\ 1 - \varkappa^2 z &= \frac{(x x_3)(x_1 x_4)}{(x x_4)(x_1 x_3)}, \end{aligned}$$

(7) $$dz = \frac{(x_4 x_1)(x_4 x_2)}{(x_2 x_1)} \frac{dx}{(x x_4)^2},$$

(8) $$\varkappa^2 = \frac{(x_3 x_4)(x_1 x_2)}{(x_1 x_3)(x_2 x_4)}, \quad \varkappa'^2 = \frac{(x_2 x_3)(x_1 x_4)}{(x_2 x_4)(x_1 x_3)}$$

und aus (3):

(9) $$\frac{\sqrt{(x_3 x_1)(x_4 x_2)}\, dx}{\sqrt{-(x_1 x)(x_2 x)(x_3 x)(x_4 x)}} = \frac{dz}{\sqrt{z(1 - z)(1 - \varkappa^2 z)}}.$$

Nach § 2 wird $\varkappa^2$ ein positiver echter Bruch, wenn die x_1, x_2, x_3, x_4, reell sind und der Größe nach zyklisch aufeinander folgen. Dies gibt also acht verschiedene solche Transformationen,

und man kann darunter je zwei auswählen, bei denen das Intervall $z = 0$ bis $z = 1$ einem gegebenen der Intervalle $(x_1 x_2)$, $(x_2 x_3)$, $(x_3 x_4)$, $(x_4 x_1)$ entspricht; dem wachsenden z entsprechen bei der einen dieser Transformationen die wachsenden x, bei der anderen die abnehmenden x (mit dem Durchgange von $+\infty$ zu $-\infty$). Im ersten Falle haben die Quadratwurzeln in (9) beiderseits das gleiche, im zweiten das entgegengesetzte Zeichen.

Wenn man nicht darauf besteht, daß $\varkappa^2$ ein positiver echter Bruch ist, so kann man die Punkte x_1, x_2, x_3, x_4 auf alle Arten permutieren und erhält 24 verschiedene lineare Transformationen in die Normalform, von denen je vier dasselbe $\varkappa^2$ ergeben; man erhält im ganzen sechs verschiedene Modulen, die nach § 2, (6) auseinander abgeleitet werden.

Man übersieht am leichtesten die Gesamtheit dieser Transformationen, wenn man annimmt, das zu transformierende Integral habe bereits die Normalform:

$$\frac{dx}{\sqrt{x(1-x)(1-\lambda^2 x)}};$$

man hat dann in den Formeln (6) bis (9) die x_1, x_2, x_3, x_4 auf alle möglichen Arten durch 0, 1, $1:\lambda^2$, ∞ zu ersetzen. Wir nehmen als Beispiel die folgenden Zuordnungen:

	x_1,	x_2,	x_3,	x_4,
1)	0,	∞,	$\frac{1}{\lambda^2}$,	1,
2)	0,	$\frac{1}{\lambda^2}$,	1,	∞,
3)	1,	0,	∞,	$\frac{1}{\lambda^2}$.

Man erhält dann aus (6) und (8)

$$1)\quad z = \frac{-x}{1-x}, \qquad \varkappa^2 = 1 - \lambda^2 = \lambda'^2,$$

$$2)\quad z = \lambda^2 x, \qquad \varkappa^2 = \frac{1}{\lambda^2},$$

$$3)\quad z = \frac{1-x}{1-\lambda^2 x}, \qquad \varkappa^2 = \lambda^2$$

und für das Differential

$$\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}}$$

ergibt sich in den drei Fällen:

$$1)\qquad \frac{dx}{\sqrt{-x(1-x)(1-\lambda^2 x)}},$$

$$2)\qquad \frac{\lambda\, dx}{\sqrt{x(1-x)(1-\lambda^2 x)}},$$

$$3)\qquad \frac{dx}{\sqrt{x(1-x)(1-\lambda^2 x)}}.$$

§ 4. Die Legendresche Normalform.

Wenn die Funktion $f(x)$, die in dem elliptischen Differential unter dem Wurzelzeichen steht, reelle Koeffizienten hat, so sind drei Fälle möglich:

1. $f(x)$ hat vier reelle Wurzeln x_1, x_2, x_3, x_4;
2. $f(x)$ hat zwei reelle Wurzeln x_1, x_2 und ein paar konjugiert imaginäre Wurzeln x_3, x_4;
3. $f(x)$ hat zwei Paare konjugiert imaginärer Wurzeln x_1, x_2 und x_3, x_4.

In allen drei Fällen läßt sich das elliptische Differential durch eine reelle lineare Transformation auf die Form bringen:

$$(1)\qquad \frac{dz}{\sqrt{(z^2-\alpha)(z^2-\beta)}},$$

worin α und β reelle (positive oder negative) Konstanten sind.

Wir bestimmen die lineare Abhängigkeit zwischen den Variablen x und z so, daß sich folgende Werte entsprechen:

$$(2)\qquad \begin{array}{ccccc} x, & x_1, & x_2, & x_3, & x_4, \\ z, & \sqrt{\alpha}, & -\sqrt{\alpha}, & \sqrt{\beta}, & -\sqrt{\beta}, \end{array}$$

und erhalten eine Substitution der Form:

$$(3)\qquad h\frac{x-x_1}{x-x_2} = \frac{z-\sqrt{\alpha}}{z+\sqrt{\alpha}}.$$

Um h zu bestimmen, setzen wir $x = x_3$, $x = x_4$ und entsprechend $z = \sqrt{\beta}$, $z = -\sqrt{\beta}$, und erhalten

$$h\frac{(x_3 x_1)}{(x_3 x_2)} = \frac{\sqrt{\beta}-\sqrt{\alpha}}{\sqrt{\beta}+\sqrt{\alpha}},\qquad h\frac{(x_4 x_1)}{(x_4 x_2)} = \frac{\sqrt{\beta}+\sqrt{\alpha}}{\sqrt{\beta}-\sqrt{\alpha}}.$$

Daraus durch Multiplikation und Division

$$(4)\qquad h = \sqrt{\frac{(x_3 x_2)(x_4 x_2)}{(x_3 x_1)(x_4 x_1)}},\qquad \frac{\sqrt{\alpha}-\sqrt{\beta}}{\sqrt{\alpha}+\sqrt{\beta}} = \sqrt{\frac{(x_3 x_1)(x_4 x_2)}{(x_3 x_2)(x_4 x_1)}}.$$

Setzen wir, wie in § 2

$$(5)\qquad \begin{aligned} a &= (x_2 x_3)(x_1 x_4), \\ b &= (x_3 x_1)(x_2 x_4), \\ c &= (x_1 x_2)(x_3 x_4), \\ a + b &+ c = 0, \end{aligned}$$

so könnnen wir, da es nur auf das Verhältnis von α zu β ankommt, die letzte der Gleichungen (4) dadurch befriedigen, daß wir setzen:

$$(6)\qquad \sqrt{\alpha} = \sqrt{\pm a} + \sqrt{\mp b}, \quad \sqrt{\beta} = \sqrt{\pm a} - \sqrt{\mp b},$$

und aus (3) ergibt sich für z der Ausdruck

$$(7)\qquad z = \sqrt{\alpha}\,\frac{(x x_2)\sqrt{(x_3 x_1)(x_4 x_1)} + (x x_1)\sqrt{(x_3 x_2)(x_4 x_2)}}{(x x_2)\sqrt{(x_3 x_1)(x_4 x_1)} - (x x_1)\sqrt{(x_3 x_2)(x_4 x_2)}}.$$

Stellt man neben (3) noch die daraus folgende Gleichung:

$$h'\frac{x - x_3}{x - x_4} = \frac{z - \sqrt{\beta}}{z + \sqrt{\beta}}$$

auf, so ergibt sich durch logarithmische Differentiation:

$$\frac{(x_1 x_2)\,dx}{(x x_1)(x x_2)} = \frac{2\sqrt{\alpha}\,dz}{z^2 - \alpha}, \quad \frac{(x_3 x_4)\,dx}{(x x_3)(x x_4)} = \frac{2\sqrt{\beta}\,dz}{z^2 - \beta},$$

und daraus durch Multiplikation mit Rücksicht auf (5) und (6):

$$(8)\qquad \frac{dx}{\sqrt{\pm (x x_1)(x x_2)(x x_3)(x x_4)}} = \frac{2\,dz}{\sqrt{(z^2 - \alpha)(z^2 - \beta)}}.$$

Wenn nun die vier Wurzeln von $f(x)$ reell sind, so gibt es, wie wir im § 2 gesehen haben, acht Arten, diese Wurzeln den Zeichen x_1, x_2, x_3, x_4 so zuzuordnen, daß a und b entgegengesetzte Zeichen haben, und wenn also $\pm a$, $\mp b$ positiv sind, so werden $\sqrt{\alpha}$, $\sqrt{\beta}$ reell, also α, β positiv, und nach (7) wird dann auch z reell.

Sind zweitens x_1, x_2 reell, x_3, x_4 konjugiert imaginär, so sind a und $-b$ konjugiert imaginär, also wird, wenn die Vorzeichen der Quadratwurzeln $\sqrt{\pm a}$, $\sqrt{\mp b}$ passend bestimmt werden, $\sqrt{\alpha}$ reell, $\sqrt{\beta}$ rein imaginär, also α positiv, β negativ und z reell [weil $(x_3 x_1)(x_4 x_1)$ und $(x_3 x_2)(x_4 x_2)$ als Produkte konjugiert imaginärer Größen positiv sind].

Sind endlich x_1, x_2 und x_3, x_4 zwei konjugiert imaginäre Paare, so sind a und $-b$ beide positiv. Nehmen wir also in (6) die unteren Zeichen, so werden $\sqrt{\alpha}$, $\sqrt{\beta}$ rein imaginär, also α und β negativ, und aus (7) ergibt sich für z ein reeller Ausdruck.

Setzt man dann

$$z^2 = y, \tag{9}$$

so ergibt sich

$$\frac{2\,dz}{\sqrt{(z^2-\alpha)(z^2-\beta)}} = \frac{dy}{\sqrt{y(y-\alpha)(y-\beta)}} \tag{10}$$

und man hat also durch die quadratische Substitution (9) ein elliptisches Differential erhalten, bei dem unter dem Wurzelzeichen eine Funktion dritten Grades mit reellen Wurzeln steht, das man nach § 3 durch lineare Substitution auf die Normalform

$$\frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}$$

bringen kann, und darin können ζ und $\varkappa$ als positive echte Brüche angenommen werden.

Die Legendresche Normalform ergibt sich daraus, wenn man

$$\zeta = \sin^2\varphi, \qquad d\zeta = 2\sin\varphi\cos\varphi\,d\varphi$$

setzt:

$$\frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}} = \frac{2\,d\varphi}{\sqrt{1-\varkappa^2\sin^2\varphi}}. \tag{11}$$

§ 5. Die Weierstrasssche Normalform.

Eine andere Normalform des elliptischen Differentials hat Weierstrass seinen Untersuchungen zugrunde gelegt, nämlich die Form

$$du = \frac{dz}{\sqrt{4z^3 - g_2 z - g_3}}, \tag{1}$$

in der g_2, g_3 Konstanten sind, die die erste und zweite Invariante des Differentials genannt werden. Das allgemeine elliptische Differential

$$\frac{dx}{\sqrt{f(x)}}, \tag{2}$$

worin

$$f(x) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 \tag{3}$$

ist, kann durch eine lineare Transformation auf die Weierstrasssche Normalform gebracht werden, wenn die Wurzeln x_1, x_2, x_3, x_4 von $f(x)$ bekannt sind. Am einfachsten geschieht dies auf folgende Weise.

Die Wurzeln der kubischen Funktion

$$\varphi(z) = 4z^3 - g_2 z - g_3$$

mögen mit e_1, e_2, e_3 bezeichnet sein. Dann ist

$$\varphi(z) = 4(z - e_1)(z - e_2)(z - e_3)$$

und $e_1 + e_2 + e_3 = 0$.

Wir lassen die Werte von x und z einander folgendermaßen entsprechen:

$$\begin{matrix} x, & x_1, & x_2, & x_3, & x_4, \\ z, & \infty, & e_1, & e_2, & e_3, \end{matrix}$$

und es ergibt sich, wenn wir mit m einen konstanten Faktor bezeichnen, der willkürlich angenommen werden kann:

$$(4) \qquad \begin{aligned} z - e_1 &= \frac{m(x x_2)}{(x_1 x_2)(x x_1)} = m\left(\frac{1}{(x_1 x_2)} - \frac{1}{(x_1 x)}\right) \\ z - e_2 &= \frac{m(x x_3)}{(x_1 x_3)(x x_1)} = m\left(\frac{1}{(x_1 x_3)} - \frac{1}{(x_1 x)}\right). \\ z - e_3 &= \frac{m(x x_4)}{(x_1 x_4)(x x_1)} = m\left(\frac{1}{(x_1 x_4)} - \frac{1}{(x_1 x)}\right) \end{aligned}$$

Der Faktor m muß in allen drei Gleichungen derselbe sein, damit die Differenzen $(z - e_3) - (z - e_2) = e_2 - e_3$ usw. von x unabhängig werden.

Bildet man diese Differenzen und setzt wie in Algebra Bd. 1, § 70

$$\begin{aligned} (x_1 x_2)(x_3 x_4) &= U, \\ (x_1 x_3)(x_4 x_2) &= V, \\ (x_1 x_4)(x_2 x_3) &= W, \end{aligned}$$

so folgt

$$e_2 - e_3 = \frac{-mU}{(x_1 x_2)(x_1 x_3)(x_1 x_4)}.$$

Führt man einen neuen willkürlichen Faktor μ ein, indem man

$$(5) \qquad m = 3\mu a_0 (x_1 x_2)(x_1 x_3)(x_1 x_4)$$

setzt, so folgt

$$e_2 - e_3 = -3\mu a_0 U, \quad e_3 - e_1 = -3\mu a_0 V, \quad e_1 - e_2 = -3\mu a_0 W$$

und daraus wegen $e_1 + e_2 + e_3 = 0$,

$$\begin{aligned} e_1 &= \mu a_0 (V - W), \\ e_2 &= \mu a_0 (W - U), \\ e_3 &= \mu a_0 (U - V). \end{aligned}$$

Die in Algebra I, § 70 eingeführten Größen y_1, y_2, y_3 sind also gleich $e_1 : \mu$, $e_2 : \mu$, $e_3 : \mu$, und man erhält nach der dortigen Formel (11) für die e_1, e_2, e_3 die kubische Gleichung:

$$z^3 - 3 A \mu^2 z + \mu^3 B = 0.$$

Es wird also, wenn $\varphi(z) = 4 z^3 - g_2 z - g_3$,

$$\varphi(z) = 4(z - e_1)(z - e_2)(z - e_3) = 4 z^3 - g_2 z - g_3$$

sein soll,

$$g_2 = 12 \mu^2 A, \qquad g_3 = -4 \mu^3 B. \tag{6}$$

Hierin sind

$$\begin{aligned} A &= a_2^2 - 3 a_1 a_3 + 12 a_0 a_4 \\ B &= 27 a_1^2 a_4 + 27 a_0 a_3^2 + 2 a_2^3 - 72 a_0 a_2 a_4 - 9 a_1 a_2 a_3 \end{aligned} \tag{7}$$

die erste und zweite Invariante der biquadratischen Form $f(x)$.

Die logarithmische Differentiation der beiden ersten Gleichungen (4) ergibt

$$\frac{d z^2}{(z - e_1)(z - e_2)} = \frac{d x^2 (x_1 x_2)(x_1 x_3)}{(x x_1)^2 (x x_2)(x x_3)},$$

und mit Hilfe der letzten Gleichung (4) nach (5):

$$\frac{d z}{\sqrt{4 z^3 - g_2 z - g_3}} = \frac{d x}{\sqrt{12 \mu f(x)}}. \tag{8}$$

Wollen wir diese Resultate auf den Fall anwenden, wo $f(x)$ die Normalform

$$f(x) = x(1 - x)(1 - \varkappa^2 x) = x - x^2(1 + \varkappa^2) + \varkappa^2 x^3$$

hat, und der Punkt $z = \infty$ dem Punkte $x = 0$ entspricht, so lassen wir a_0 in Null, x_4 in Unendlich übergehen, aber das Produkt $a_0 x_4$ in einen endlichen Wert, den wir $= 1$ annehmen können.

Es wird dann

$$\begin{aligned} a_0 x_4 &= 1, & a_0 &= 0, & a_1 &= \varkappa^2, \\ a_2 &= -(1 + \varkappa^2), & a_3 &= 1, & a_4 &= 0 \end{aligned}$$

und folglich

$$\begin{aligned} A &= (1 + \varkappa^2)^2 - 3 \varkappa^2 = 1 - \varkappa^2 + \varkappa^4 = 1 - \varkappa^2 \varkappa'^2 \\ B &= -(1 + \varkappa^2)[2(1 + \varkappa^2)^2 - 9 \varkappa^2] \\ &= -(1 + \varkappa^2)(2 - \varkappa^2)(1 - 2 \varkappa^2) \\ &= (1 + \varkappa^2)(1 + \varkappa'^2)(\varkappa^2 - \varkappa'^2) \\ &= (2 + \varkappa^2 \varkappa'^2)(\varkappa^2 - \varkappa'^2), \end{aligned}$$

wenn $\varkappa'^2 = 1 - \varkappa^2$ gesetzt ist.

Es wird also, wenn wir noch die Diskriminante

$$\varDelta = 16.27\mu^6(4A^3 - B^2)$$

beifügen

$$(9)\qquad \begin{aligned} g_2 &= 12\mu^2(1 - \varkappa^2\varkappa'^2),\\ g_3 &= -4\mu^3(2 + \varkappa^2\varkappa'^2)(\varkappa^2 - \varkappa'^2),\\ \varDelta &= g_2^3 - 27g_3^2 = 27^2.16\mu^6\varkappa^4\varkappa'^4, \end{aligned}$$

und man erhält aus (6) die Transformation

$$(10)\qquad \frac{dz}{\sqrt{4z^3 - g_2 z - g_3}} = \frac{dx}{\sqrt{12\mu x(1-x)(1-\varkappa^2 x)}};$$

um die Substitution zu finden, setzen wir $x_1 = 0$, $x_2 = 1$, $x_3 = 1:\varkappa^2$, $x_4 = \infty$, $a_0 z_4 = 1$ und erhalten

$$a_0 U = 1, \quad a_0 V = \frac{-1}{\varkappa^2}, \quad a_0 W = \frac{\varkappa'^2}{\varkappa^2},$$

folglich

$$e_1 = \mu\frac{\varkappa^2 - 2}{\varkappa^2}, \quad e_2 = \mu\frac{1 - 2\varkappa^2}{\varkappa^2}, \quad e_3 = \mu\frac{1 + \varkappa^2}{\varkappa^2}$$

$$(11)\qquad z = \frac{3\mu}{\varkappa^2}\left(\frac{\varkappa^2+1}{3} - \frac{1}{x}\right).$$

Bei dieser Transformation des elliptischen Differentials in der Weierstrassschen Normalform wird die Zerlegung der Funktion $f(x)$ in ihre linearen Faktoren, also die Auflösung der biquadratischen Gleichung $f(x) = 0$, vorausgesetzt. Eine andere, freilich nicht lineare Transformation, die ohne diese Voraussetzung den gleichen Zweck erreicht, hat Hermite gegeben (Crelles Journal, Bd. 52). Um sie darzustellen, benutzen wir die homogene Form des elliptischen Differentials

$$(12)\qquad \frac{y\,dx - x\,dy}{\sqrt{f(x,y)}},$$

worin

$$(13)\qquad f(xy) = a_0x^4 + a_1x^3y + a_2x^2y^2 + a_3xy^3 + a_4y^4.$$

Diese biquadratische Form hat außer den beiden Invarianten A, B noch zwei Kovarianten:

$$(14)\qquad \begin{aligned} H &= \frac{1}{3}\left[\frac{\partial^2 f}{\partial x^2}\frac{\partial^2 f}{\partial y^2} - \left(\frac{\partial^2 f}{\partial x\,\partial y}\right)^2\right]\\ T &= \frac{1}{12}\left(\frac{\partial f}{\partial x}\frac{\partial H}{\partial y} - \frac{\partial f}{\partial y}\frac{\partial H}{\partial x}\right), \end{aligned}$$

wo H und T Formen vierten und sechsten Grades sind, deren Koeffizienten sich rational und mit ganzzahligen Zahlenkoeffizienten aus den Koeffizienten von f zusammensetzen. Zwischen diesen Formen besteht dann noch die Relation

(15) $$H^3 - 48AHf^2 - 64Bf^3 = -27T^2$$

(Bd. I, § 70, 72).

Es ist aber nach dem Eulerschen Satz über homogene Funktionen

$$4f = \frac{\partial f}{\partial x}x + \frac{\partial f}{\partial y}y, \quad df = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy,$$
$$4H = \frac{\partial H}{\partial x}x + \frac{\partial H}{\partial y}y, \quad dH = \frac{\partial H}{\partial x}dx + \frac{\partial H}{\partial y}dy,$$

woraus

$$f\,dH - H\,df = -3T(y\,dx - x\,dy),$$

und wenn also nach (15)

(16) $$3\sqrt{3}\,T = \sqrt{-H^3 + 48Af^2H + 64Bf^3}$$

gesetzt wird:

$$\frac{y\,dx - x\,dy}{\sqrt{f}} = \frac{-\sqrt{3}(f\,dH - H\,df)}{\sqrt{-(H^3 - 48Af^2H - 64Bf^3)f}}.$$

Macht man nun die Substitution

(17) $$z = -\frac{\mu H}{4f}$$

mit einem unbestimmten Faktor μ, so ergibt sich

(18) $$\frac{y\,dx - x\,dy}{\sqrt{3\mu f}} = \frac{dz}{\sqrt{4z^3 - g_2 z - g_3}},$$

wenn wie früher

(19) $$g_2 = 12\mu^2 A, \quad g_3 = -4\mu^3 B.$$

Man kann diese Transformation auf ein Differential anwenden, das schon die Normalform hat. Setzt man

$$f(x, y) = 4x^3y - g_2xy^3 - g_3y^4,$$

so hat man

a_0	a_1	a_2	a_3	a_4

durch

0	4	0	$-g_2$	$-g_3$

zu ersetzen, und es ergibt sich aus (7)

$$A = 12g_2, \quad B = -27.16g_3.$$

Wenn man also $\mu = \frac{1}{12}$ setzt, so gehen die Gleichungen (19) in die Identitäten $g_2 = g_2$, $g_3 = g_3$ über.

Wenn man dann $y = 1$ setzt, so ergibt die Transformation (18)

$$(20) \qquad \frac{2\,dx}{\sqrt{4x^3 - g_2 x - g_3}} = \frac{dz}{\sqrt{4z^3 - g_2 z - g_3}}.$$

Diese Transformation wird nach (16) durch

$$z = \frac{-H}{48 f}$$

vermittelt. Es ergibt sich aber aus (14):

$$H = -48\,[(x^2 + \tfrac{1}{4} g_2)^2 + 2 g_3 x],$$

und folglich erhalten wir

$$(21) \qquad z = \frac{(x^2 + \frac{1}{4} g_2)^2 + 2 g_3 x}{4x^3 - g_2 x - g_3}.$$

Weiter ergibt sich noch aus (14)

$$T = 64x^6 - 80 g_2 x^4 - 320 g_3 x^3 - 20 g_2^2 x^2 - 16 g_2 g_3 x + g_2^3 - 32 g_3^2$$

und dann nach (16)

$$(22) \qquad 4\sqrt{4x^3 - g_2 x - g_3}^{\,3} \sqrt{4z^3 - g_2 z - g_3} = T.$$

Durch (20), (21), (22) ist die Multiplikation des elliptischen Differentials mit 2 geleistet. Es ist dadurch nicht nur z als eindeutige (rationale) Funktion von x dargestellt, sondern auch die eine Quadratwurzel eindeutig durch die andere, d. h. es ist einem Punkte x eindeutig ein Punkt z zugeordnet.

§ 6. Elliptische Kurven.

Jede algebraische Abhängigkeit zwischen zwei Veränderlichen x, y wird ausgedrückt durch eine Gleichung der Form

$$(1) \qquad F(x, y) = 0,$$

worin $F(x, y)$ eine ganze Funktion der beiden Veränderlichen x, y bezeichnet. Betrachtet man x und y als Cartesische Koordinaten eines Punktes in der Ebene, so ist (1) die Gleichung einer Kurve $n$ten Grades, wenn F in bezug auf x und y zusammengenommen von der $n$ten Dimension ist. Diese Kurve ist dann das geometrische Bild der algebraischen Abhängigkeit, wobei indessen auch imaginäre Punkte mit berücksichtigt werden müssen.

Ist dann $\Phi(x,y)$ eine ganze oder gebrochene rationale Funktion von x und y, und y von x durch die Gleichung (1) abhängig, so sind

(2) $$\Phi(x,y)\,dx, \qquad \int \Phi(x,y)\,dx$$

die zu der Kurve F gehörigen algebraischen Differentiale und Integrale.

Beispielsweise ist, wenn $f(x)$ eine Funktion dritten oder vierten Grades von x ist,

$$y^2 - f(x) = 0$$

die Gleichung einer Kurve dritten oder vierten Grades, zu der die mit der Irrationalität $\sqrt{f(x)}$ behafteten elliptischen Differentiale und Integrale gehören.

Wir wollen hier alle Kurven, deren Differentiale und Integrale auf elliptische reduzierbar sind, elliptische Kurven nennen. Wie das Beispiel zeigt, kommen darunter Kurven dritten und vierten Grades vor.

Kegelschnitte gehören nicht zu den elliptischen Kurven, weil, wenn zwischen x und y eine Gleichung zweiten Grades besteht, x und y als rationale Funktionen eines Parameters t dargestellt werden können, wodurch das algebraische Differential auf ein rationales nach t zurückgeführt werden kann. Solche Kurven heißen rationale Kurven.

Wir werden sehen, daß alle Kurven dritten Grades ohne Doppel- oder Rückkehrpunkt zu den elliptischen gehören. Kurven höheren Grades können nur dann dazu gehören, wenn sie eine gewisse Anzahl singulärer Punkte haben. Dies ist ein fundamentales Kapitel in der allgemeinen Theorie der algebraischen Funktionen, das nicht in den Plan dieses Werkes gehört[1]).

---

[1]) Die wichtigsten diesen Gegenstand betreffenden Arbeiten sind:

Riemann, Theorie der Abelschen Funktionen [Crelles Journal, Bd. 54 (1857)]. Mathematische Werke, 2. Aufl., S. 88, 487. Nachträge, herausgegeben von Noether und Wirtinger (1902).

Aronhold, Monatsberichte der Berliner Akademie vom 25. April 1861.

Clebsch, Über die Anwendung der Abelschen Funktionen in der Geometrie (Crelles Journal, Bd. 63).

Clebsch, Über diejenigen ebenen Kurven, deren Koordinaten rationale Funktionen eines Parameters sind (ibid., Bd. 64).

Clebsch, Über diejenigen Kurven, deren Koordinaten sich als elliptische Funktionen eines Parameters darstellen lassen (ibid., Bd. 64).

Für die Untersuchung algebraischer Differentiale von diesem Gesichtspunkte ist die Einführung **homogener Variablen** zweckmäßig. Wir setzen $x = x_1 : x_3$, $y = x_2 : x_3$, $x_3^n F(x, y) = f(x_1, x_2, x_3)$ dann ist $f(x_1, x_2, x_3)$ eine **homogene Funktion** $n$ter Ordnung der drei Veränderlichen x_1, x_2, x_3 und

$$(3) \qquad f(x_1, x_2, x_3) = 0$$

die Gleichung einer Kurve $n$ter Ordnung in homogenen Koordinaten. Es wird

$$dx = \frac{x_3\,dx_1 - x_1\,dx_3}{x_3^2}$$

und

$$(4) \qquad d\Omega = \Phi(x, y)\,dx = \frac{1}{x_3^2}\,\Phi\left(\frac{x_1}{x_3}, \frac{x_2}{x_3}\right)(x_3\,dx_1 - x_1\,dx_3).$$

Nun ist aber nach dem **Eulerschen** Satz über homogene Funktionen, wenn wir mit f_1, f_2, f_3 die partiellen Ableitungen von f nach x_1, x_2, x_3 bezeichnen,

$$\begin{aligned} f_1 x_1 + f_2 x_2 + f_3 x_3 &= 0, \\ f_1\,dx_1 + f_2\,dx_2 + f_3\,dx_3 &= 0, \end{aligned}$$

daher, wenn ϱ einen Proportionalitätsfaktor bedeutet,

$$\begin{aligned} f_1 &= \varrho\,(x_2\,dx_3 - x_3\,dx_2), \\ f_2 &= \varrho\,(x_3\,dx_1 - x_1\,dx_3), \\ f_3 &= \varrho\,(x_1\,dx_2 - x_2\,dx_1), \end{aligned}$$

und wenn man mit c_1, c_2, c_3 ganz willkürliche Größen, z. B. Konstanten, bezeichnet:

$$c_1 f_1 + c_2 f_2 + c_3 f_3 = \varrho\,\Sigma \pm c_1\,x_2\,dx_3,$$

wenn $\Sigma \pm c_1\,x_2\,dx_3$ in üblicher Weise die Determinante

$$\begin{vmatrix} c_1 & c_2 & c_3 \\ x_1 & x_2 & x_3 \\ dx_1 & dx_2 & dx_3 \end{vmatrix}$$

bedeutet. Es folgt also:

$$x_3\,dx_1 - x_1\,dx_3 = \frac{f_2\,\Sigma \pm c_1\,x_2\,dx_3}{c_1 f_1 + c_2 f_2 + c_3 f_3},$$

und wenn man

$$\frac{f_2}{x_3^2}\,\Phi\left(\frac{x_1}{x_4}, \frac{x_2}{x_3}\right) = \Psi$$

Brill, Über diejenigen Kurven, deren Koordinaten sich als hyperelliptische Funktionen eines Parameters darstellen lassen (ibid., Bd. 65).
Clebsch und Gordan, Theorie der Abelschen Funktionen (Teubner, Leipzig 1866).

setzt, so ergibt sich aus (4) der Ausdruck für das allgemeinste zu der Kurve f gehörige algebraische Differential:

$$d\Omega = \frac{\Psi \Sigma \pm c_1 x_2 dx_3}{c_1 f_1 + c_2 f_2 + c_3 f_3}, \tag{5}$$

worin Ψ eine ganze oder gebrochene homogene Funktion der $(n-3)$ten Ordnung ist. Die willkürlichen Größen c_1, c_2, c_3 kommen nur scheinbar in diesem Ausdruck vor. In Wirklichkeit ist er davon ganz unabhängig.

Wir betrachten wieder den Fall $n = 3$. Dann ist der einfachste Fall der, daß Ψ eine Konstante ist, und (5) geht dann in das elliptische Differential erster Gattung über:

$$du = \frac{\Sigma \pm c_1 x_2 dx_3}{c_1 f_1 + c_2 f_2 + c_3 f_3}. \tag{6}$$

Dieses wollen wir nun mit Hilfe der Kovarianten der ternären Form dritten Grades auf die Weierstrassche Form transformieren.

Wir haben Bd. II, § 107 die fundamentalen Kovarianten der kubischen Form kennen gelernt. Es waren dies außer f selbst:

$$\Delta = \frac{1}{6^3}\begin{vmatrix} f_{11}, & f_{12}, & f_{13} \\ f_{21}, & f_{22}, & f_{23} \\ f_{31}, & f_{32}, & f_{33} \end{vmatrix}, \quad J = \frac{1}{36}\begin{vmatrix} f_{11}, & f_{12}, & f_{13}, & \Delta_1 \\ f_{21}, & f_{22}, & f_{23}, & \Delta_2 \\ f_{31}, & f_{32}, & f_{33}, & \Delta_3 \\ \Delta_1, & \Delta_2, & \Delta_3, & 0 \end{vmatrix},$$

$$K = \frac{1}{9}\begin{vmatrix} f_1, & \Delta_1, & J_1 \\ f_2, & \Delta_2, & J_2 \\ f_3, & \Delta_3, & J_3 \end{vmatrix},$$

wobei die Indizes 1, 2, 3 die Differentiation nach den Variablen x_1, x_2, x_3 bedeuten.

Es folgt aus dem Multiplikationssatz der Determinanten, da f und $df = 0$ sind:

$$\begin{vmatrix} c_1, & c_2, & c_3 \\ x_1, & x_2, & x_3 \\ dx_1, & dx_2, & dx_3 \end{vmatrix} \begin{vmatrix} f_1, & f_2, & f_3 \\ \Delta_1, & \Delta_2, & \Delta_3 \\ J_1, & J_2, & J_3 \end{vmatrix} = \begin{vmatrix} \Sigma x_i \Delta_i, & d\Delta \\ \Sigma x_i J_i, & dJ \end{vmatrix} \Sigma c_i f_i$$

$$= 3\,\Sigma c_i f_i (\Delta\, dJ - 2J d\Delta),$$

und daraus

$$du = 3\frac{\Delta\, dJ - 2 J d\Delta}{K}. \tag{7}$$

Mit Hilfe der Kovarianten haben wir die Form $f(x)$ auf die kanonische Form

$$\varphi(y) = y_1^3 + y_2^3 + y_3^3 + 6 m y_1 y_2 y_3$$

reduziert.

Wir haben, wenn r die Substitutionsdeterminante bedeutet:

$$P = \frac{(2 + m^3) m^3 f^2 + (2 - 5 m^3) m r^2 f \varDelta + 3 m^2 r^4 \varDelta^2 - r^6 J}{(1 + 8 m^3)^2},$$

$$Q = \frac{(1 + 2 m^3) f - 6 m r^2 \varDelta}{1 + 8 m^3},$$

$$R = \frac{m^2 f + r^2 \varDelta}{1 + 8 m^3}$$

gesetzt und erhielten y_1^3, y_2^3, y_3^3 als Wurzeln der kubischen Gleichung

$$u^3 - Q u^2 + P u - R^3 = 0,$$

und die Diskriminante dieser kubischen Gleichung ist

$$D_1 = \frac{r^{18} K^2}{(1 + 8 m^3)^6}.$$

Drückt man diese Diskriminante durch P, Q, R aus, so erhält man K^2 rational durch f, $\varDelta$, J dargestellt. Wir haben an der erwähnten Stelle der Algebra diesen Ausdruck nicht explizite angegeben. Jetzt müssen wir ihn aber bilden, wenn auch nur unter der Voraussetzung $f = 0$, d. h. nur für die Punkte der Kurve. Es ist aber [nach Bd. I, § 50, (10)]

$$D_1 = P^2 Q^2 + 18 P Q R^3 - 4 P^3 - 4 Q^3 R^3 - 27 R^6.$$

Darin hat man zu setzen:

$$P = \frac{3 m^2 r^4 \varDelta^2 - r^6 J}{(1 + 8 m^3)^2}, \quad Q = \frac{-6 m r^2 \varDelta}{1 + 8 m^3}, \quad R = \frac{r^2 \varDelta}{1 + 8 m^3},$$

und man erhält durch eine nicht schwierige Rechnung, wenn man mit S und T die beiden Invarianten der Kurve dritter Ordnung bezeichnet (Bd. II, § 108),

$$(1 + 8 m^3)^6 D_1 = r^{18}(4 J^3 + 108 S J \varDelta^4 - 27 T \varDelta^6),$$

und folglich

(8) $$K^2 = 4 J^3 + 108 S J \varDelta^4 - 27 T \varDelta^6.$$

Diese Gleichung ist aber nicht identisch, sondern nur unter der Voraussetzung $f = 0$ befriedigt. Der vollständige Ausdruck von K^2 durch J, $\varDelta$, f wird sehr viel komplizierter.

Setzt man

(9) $$\frac{J}{\varDelta^2} = 3z, \quad dz = \frac{1}{3}\frac{\varDelta dJ - 2Jd\varDelta}{\varDelta^3},$$

so ergibt sich aus (8)

$$K^2 = 27\varDelta^6(4z^3 + 12Sz - T)$$

und aus (7)

(10) $$du = \frac{1}{\sqrt{3}}\frac{dz}{\sqrt{4z^3 + 12Sz - T}},$$

und dies ist die Weierstrassche Normalform für $g_2 = -12S$, $g_3 = T$.

§ 7. Elliptische Raumkurven vierter Ordnung.

Man kann algebraische Funktionen einer Veränderlichen auch durch Gleichungen zwischen mehreren Variablen darstellen, wenn man die Anzahl der Gleichungen entsprechend vergrößert. Nimmt man z. B. drei Variable x, y, z und läßt zwischen ihnen zwei Gleichungen

(1) $$\varphi(x,y,z) = 0, \qquad \psi(x,y,z) = 0$$

bestehen, so kann man aus diesen beiden Gleichungen z. B. x eliminieren und erhält eine Gleichung zwischen y und z, durch die y als algebraische Funktion von z definiert ist. Es kann dann, wenn man gewisse Ausnahmefälle ausschließt, x und jede rationale Funktion von x, y, z rational durch y und z dargestellt werden. Die Integrale der Form

(2) $$\int F(x,y,z)\,dz,$$

in denen F eine rationale Funktion bedeutet, gehören dann zu dem durch (1) dargestellten algebraischen Gebilde. Nimmt man x, y, z als Cartesische Koordinaten im Raume an, so stellt (1) eine Raumkurve als den Durchschnitt zweier Flächen $\varphi = 0$, $\psi = 0$ dar, und die Integrale (2) gehören zu dieser Raumkurve. Die Kurve heißt wieder elliptisch, wenn diese Integrale elliptisch sind.

Wir wollen diese Betrachtungen auf die Raumkurven vierter Ordnung erster Spezies anwenden, d. h. auf die Kurven vierter Ordnung, die sich als vollständiger Durchschnitt zweier Flächen zweiten Grades darstellen lassen.

Wir führen wieder homogene Koordinaten x_1, x_2, x_3, x_4 ein und nehmen die Gleichungen zweier gegebenen Flächen zweiten Grades in der Form an:

$$(3)\qquad \begin{aligned} \varphi(x_1, x_2, x_3, x_4) &= \Sigma a_{ik} x_i x_k, \\ \psi(x_1, x_2, x_3, x_4) &= \Sigma b_{ik} x_i x_k. \end{aligned}$$

Die beiden Flächen bestimmen ein Flächenbüschel zweiter Ordnung $\xi\varphi = \eta\psi$. Alle Flächen des Büschels schneiden sich in einer Raumkurve vierter Ordnung, die wir die Grundkurve nennen. Man erhält dieselbe Kurve und dasselbe Büschel, wenn man die Funktionen φ und ψ durch φ', ψ' ersetzt, die aus φ, ψ mittels der linearen Substitution $\begin{pmatrix} m & n \\ p & q \end{pmatrix}$, also durch

$$(4)\qquad \begin{aligned} \varphi' &= m\varphi + n\psi, \\ \psi' &= p\varphi + q\psi \end{aligned}$$

abgeleitet wird, deren Determinante $r = mq - np$ von Null verschieden ist. Dadurch ergibt sich die Identität

$$(5)\qquad \xi\varphi + \eta\psi = \xi'\varphi' + \eta'\psi',$$

worin

$$(6)\qquad \begin{aligned} \xi &= m\xi' + p\eta', \\ \eta &= n\xi' + q\eta' \end{aligned}$$

eine lineare Transformation der Variablen ξ, η darstellt. Außer dieser binären Substitution kommt noch eine lineare quaternäre Substitution der Variablen x_1, x_2, x_3, x_4 (Koordinatentransformation) in Betracht, deren Determinante wir $= 1$ annehmen können.

Jede quadratische Form besitzt diesen letzteren Transformationen gegenüber eine Invariante, nämlich die Hessesche Determinante (Bd. I, § 62, 63, 66), und wir erhalten also als Invariante der Form (5):

$$(7)\qquad \begin{aligned} &f(\xi, \eta) = \\ &\Sigma \pm (\xi a_{11} + \eta b_{11})(\xi a_{22} + \eta b_{22})(\xi a_{33} + \eta b_{33})(\xi a_{44} + \eta b_{44}). \end{aligned}$$

Dies ist eine binäre biquadratische Form der Variablen ξ, η, die wir, entwickelt, so darstellen:

$$(8)\qquad f(\xi, \eta) = a_0\xi^4 + a_1\xi^3\eta + a_2\xi^2\eta^2 + a_3\xi\eta^3 + a_4\eta^4.$$

Die Koeffizienten dieser biquadratischen Form a_0, a_1, a_2, a_3, a_4 ändern sich nicht bei einer Koordinatentransformation. Sie heißen daher simultane Invarianten des Formenpaares φ, ψ (a_0 und a_4 sind die Determinanten von φ und von ψ).

Die a_i ändern sich, wenn man die ξ, η einer Substitution (6) unterwirft. Bildet man aber die Invarianten der Form (8) (nach Algebra, Bd. I, § 70), so erhält man Funktionen der Koeffizienten, die auch diesen Substitutionen gegenüber invariant sind, die also nicht zu den individuellen Formen φ, ψ, sondern zu dem ganzen Büschel und also auch zu ihrem Durchschnitt, der Grundkurve, gehören. Wir nennen sie Invarianten der Grundkurve. In bezug auf das Formensystem φ, ψ werden sie auch Kombinanten genannt. Die Grundkurve hat also zwei Invarianten:

$$(9)\quad \begin{aligned} A &= a_2^2 - 3\,a_1 a_3 + 12\,a_0 a_4, \\ B &= 27\,a_1^2 a_4 + 27\,a_0 a_3^2 + 2\,a_2^3 - 72\,a_0 a_2 a_4 - 9\,a_1 a_2 a_3, \end{aligned}$$

aus denen man die Diskriminante D nach der Formel

$$(10)\qquad 27\,D = 4\,A^3 - B^2$$

ableitet. In bezug auf die Koeffizienten von φ und ψ sind die Invarianten A, B, D von den Graden 8, 12, 24.

Das Formensystem φ, ψ hat zwei simultane quadratische Kovarianten, die man ebenso wie die Kovariante C (in Algebra I, § 65) ableitet. Die erste von ihnen ist, wenn wir $\psi_1 = \frac{1}{2}\frac{\partial \psi}{\partial x_1}, \ldots$ setzen:

$$(11)\qquad \Phi = \begin{vmatrix} a_{11}, & a_{12}, & a_{13}, & a_{14}, & \psi_1 \\ a_{21}, & a_{22}, & a_{23}, & a_{24}, & \psi_2 \\ a_{31}, & a_{32}, & a_{33}, & a_{34}, & \psi_3 \\ a_{41}, & a_{42}, & a_{43}, & a_{44}, & \psi_4 \\ \psi_1, & \psi_2, & \psi_3, & \psi_4, & 0 \end{vmatrix}$$

und die zweite Ψ erhält man daraus, indem man a_{ik} mit b_{ik} und ψ mit φ vertauscht.

Die Gleichung $\Phi = 0$ drückt eine Fläche zweiten Grades aus (die nicht zum Büschel gehört), die der geometrische Ort der Punkte x ist, deren Polaren in bezug auf ψ die Fläche φ berühren.

Wir nehmen jetzt an, daß die Diskriminante D von Null verschieden ist. Dann lassen sich die beiden Funktionen φ, ψ simultan in die Summe von vier Quadraten transformieren:

$$(12)\quad \begin{aligned} \varphi &= \alpha_1 y_1^2 + \alpha_2 y_2^2 + \alpha_3 y_3^2 + \alpha_4 y_4^2, \\ \psi &= \beta_1 y_1^2 + \beta_2 y_2^2 + \beta_3 y_3^2 + \beta_4 y_4^2, \end{aligned}$$

worin die y_i lineare Funktionen der x_i sind. Dies ist die kanonische Form des Funktionenpaares. Es wird dann:

$$(13)\quad f(\xi,\eta) = (\xi\alpha_1 + \eta\beta_1)(\xi\alpha_2 + \eta\beta_2)(\xi\alpha_3 + \eta\beta_3)(\xi\alpha_4 + \eta\beta_4),$$

und die Funktionen Φ, Ψ erhalten die kanonische Form:

$$\text{(14)}\qquad \begin{aligned}\Phi &= \Sigma\, \beta_1^2 \alpha_2 \alpha_3 \alpha_4 y_1^2,\\ \Psi &= \Sigma\, \alpha_1^2 \beta_2 \beta_3 \beta_4 y_1^2.\end{aligned}$$

Die Determinante des Systems (12), (14), als lineare Gleichungen für y_1^2, y_2^2, y_3^2, y_4^2 betrachtet, ist

$$\text{(15)}\qquad \begin{vmatrix} \alpha_1^2\beta_2\beta_3\beta_4, & \alpha_2^2\beta_1\beta_3\beta_4, & \alpha_3^2\beta_1\beta_2\beta_4, & \alpha_4^2\beta_1\beta_2\beta_3 \\ \beta_1^2\alpha_2\alpha_3\alpha_4, & \beta_2^2\alpha_1\alpha_3\alpha_4, & \beta_3^2\alpha_1\alpha_2\alpha_4, & \beta_4^2\alpha_1\alpha_2\alpha_3 \\ \alpha_1, & \alpha_2, & \alpha_3, & \alpha_4 \\ \beta_1, & \beta_2, & \beta_3, & \beta_4 \end{vmatrix}.$$

Sie verschwindet, wenn $\alpha_1 : \alpha_2 = \beta_1 : \beta_2$ wird, weil dann die beiden ersten Kolonnen miteinander proportional werden, und ebenso wenn $\alpha_i : \alpha_k = \beta_i : \beta_k$ wird. Es ist daher (15) als ganze Funktion der α, β betrachtet, teilbar durch

$$\text{(16)}\qquad \alpha_i \beta_k - \alpha_k \beta_i = (\alpha_i \beta_k),$$

und folglich auch durch das Produkt aller dieser Faktoren

$$\text{(17)}\qquad (\alpha_1\beta_2)(\alpha_1\beta_3)(\alpha_1\beta_4)(\alpha_2\beta_3)(\alpha_2\beta_4)(\alpha_3\beta_4) = \varDelta.$$

Aus der Vergleichung der Grade ergibt sich, daß sich die beiden Funktionen (15), (17) nur durch einen Zahlenfaktor unterscheiden können, und dieser ergibt sich aus der Annahme $\beta_1 = 0$, $\alpha_2 = 0$, $\alpha_4 = 0$ gleich 1. Die Determinante (15) ist also dem Produkt $\varDelta$ gleich, und das Quadrat von $\varDelta$ ist die Diskriminante D der Funktion $f(\xi, \eta)$, also gleich der Funktion D, von der wir angenommen haben, daß sie von Null verschieden sei. Es lassen sich also die y_1^2, y_2^2, y_3^2, y_4^2 linear durch φ, ψ, Φ, Ψ darstellen.

Die Kovarianten Φ, Ψ ändern sich, wenn φ und ψ nach (4) durch φ', ψ' ersetzt werden. Sie gehören also nicht zu der Grundkurve, sondern zu dem Formenpaar φ, ψ. Aber es gehen bei dieser Substitution Φ und Ψ als lineare Funktionen von y_1^2, y_2^2, y_3^2, y_4^2 in lineare Funktionen von φ, ψ, Φ, Ψ über. Diese Ausdrücke sind ziemlich kompliziert. Wir brauchen sie hier aber nur für die Punkte der Grundkurve, also für $\varphi = 0$, $\psi = 0$, und unter dieser Voraussetzung werden sie sehr einfach. Es ist da nämlich

$$\text{(18)}\qquad \begin{aligned}\Phi' &= \Sigma(p\alpha_1 + q\beta_1)^2(m\alpha_2 + n\beta_2)(m\alpha_3 + n\beta_3)(m\alpha_4 + n\beta_4)\,y_1^2,\\ \Psi' &= \Sigma(m\alpha_1 + n\beta_1)^2(p\alpha_2 + q\beta_2)(p\alpha_3 + q\beta_3)(p\alpha_4 + q\beta_4)\,y_1^2,\end{aligned}$$

und daraus ist nach (12) und (14) abzuleiten:

$$\Phi' = M\Phi + N\Psi,$$
$$\Psi' = P\Phi + Q\Psi,$$

worin die Koeffizienten M, N, P, Q noch zu bestimmen sind. Wir können dies durch Rechnung ausführen. Ohne Rechnung ergibt sich das Resultat auf folgendem Wege:

Die M, N sind ganze Funktionen zweiten Grades von p, q und dritten Grades von m, n. Nimmt man $p:q = m:n$, also $r = mq - np = 0$, so gehen Φ' und $\frac{\partial \Phi'}{\partial p}$ nach (18) in lineare Verbindungen von φ und ψ über und verschwinden also. Daraus folgt, daß M und N durch r^2 teilbar sind, und die Quotienten sind lineare Funktionen von m und n. Da aber für die beiden Fälle $\begin{pmatrix} m & n \\ p & q \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ Φ' in Φ und in Ψ übergehen muß, und da man dieselbe Betrachtung auf Ψ' anwenden kann, so folgt:

$$(19) \qquad \begin{aligned} \Phi' &= r^2(m\Phi + n\Psi), \\ \Psi' &= r^2(p\Phi + q\Psi). \end{aligned}$$

Es werden also (von dem Faktor r^2 abgesehen) die Funktionen Φ, Ψ mit den φ, ψ kongredient transformiert. (Über die strenge Begründung dieser Schlüsse sehe man Bd. I, § 20.)

Aus diesen Ergebnissen können wir auf einfache Weise, immer unter der Voraussetzung $\varphi = 0$, $\psi = 0$, die y_i^2 durch Φ und Ψ ausdrücken, also die linearen Gleichungen (12), (14) auflösen. Wenn wir nämlich die Formeln (19) auf die Substitution

$$\begin{pmatrix} m, & n \\ p, & q \end{pmatrix} = \begin{pmatrix} \beta_1, & -\alpha_1 \\ 0, & 1 \end{pmatrix}$$

anwenden, so ist $r = \beta_1$, die Funktion ψ' bleibt ungeändert $= \psi$ und φ' geht aus φ hervor, wenn

$$\alpha_1, \quad \alpha_2, \quad \alpha_3, \quad \alpha_4$$

durch

$$0, \quad (\alpha_2\beta_1), \quad (\alpha_3\beta_1), \quad (\alpha_4\beta_1)$$

ersetzt werden. Es wird also nach (14)

$$\Phi' = \beta_1^2(\alpha_2\beta_1)(\alpha_3\beta_1)(\alpha_4\beta_1)y_1^2$$

und folglich nach (19):

$$(20) \qquad \begin{aligned} (\alpha_2\beta_1)(\alpha_3\beta_1)(\alpha_4\beta_1)y_1^2 &= \alpha_1\Phi - \beta_1\Psi, \\ (\alpha_1\beta_2)(\alpha_3\beta_2)(\alpha_4\beta_2)y_2^2 &= \alpha_2\Phi - \beta_2\Psi, \\ (\alpha_1\beta_3)(\alpha_2\beta_3)(\alpha_4\beta_3)y_3^2 &= \alpha_3\Phi - \beta_3\Psi, \\ (\alpha_1\beta_4)(\alpha_2\beta_4)(\alpha_3\beta_4)y_4^2 &= \alpha_4\Phi - \beta_4\Psi. \end{aligned}$$

Das Produkt des konstanten Faktors auf der linken Seite ist die Diskriminante D, und man erhält also nach (13)

$$\text{(21)}\quad \begin{aligned} D y_1^2 y_2^2 y_3^2 y_4^2 &= f(\Phi, -\Psi) \\ &= a_0 \Phi^4 - a_1 \Phi^3 \Psi + a_2 \Phi^2 \Psi^2 - a_3 \Phi \Psi^3 + a_4 \Psi^4, \end{aligned}$$

und die y_i^2 sind also die linearen Faktoren dieser biquadratischen Form.

Es gibt noch eine weitere simultane Kovariante der Form φ, ψ, nämlich die Jacobische Funktionaldeterminante der vier Funktionen φ, ψ, Φ, Ψ. Wir bezeichnen sie so:

$$\text{(22)}\qquad K = \begin{vmatrix} \varphi_1, & \varphi_2, & \varphi_3, & \varphi_4 \\ \psi_1, & \psi_2, & \psi_3, & \psi_4 \\ \Phi_1, & \Phi_2, & \Phi_3, & \Phi_4 \\ \Psi_1, & \Psi_2, & \Psi_3, & \Psi_4 \end{vmatrix}.$$

Bildet man sie für die kanonische Form, so ergibt sich nach (12), (14), (15)

$$K = -\Delta y_1 y_2 y_3 y_4,$$

und da $\Delta^2 = D$ ist:

$$K^2 = D y_1^2 y_2^2 y_3^2 y_4^2,$$

also haben wir nach (21)

$$\text{(23)}\qquad K^2 = f(\Phi, -\Psi).$$

Die biquadratische Form $f(\Phi, -\Psi)$ hat zwei Kovarianten, die wir wie in Bd. I, § 70 so bezeichnen:

$$\text{(24)}\qquad \begin{aligned} H &= \frac{1}{3} \begin{vmatrix} \dfrac{\partial^2 f}{\partial \Phi^2}, & -\dfrac{\partial^2 f}{\partial \Phi \partial \Psi} \\ \dfrac{\partial^2 f}{\partial \Psi \partial \Phi}, & -\dfrac{\partial^2 f}{\partial \Psi^2} \end{vmatrix}, \\ T &= \frac{1}{12} \begin{vmatrix} f'(\Phi), & f'(-\Psi) \\ H'(\Phi), & H'(-\Psi) \end{vmatrix}. \end{aligned}$$

Sie sind vom vierten und sechsten Grade in der Φ, Ψ, also vom achten und zwölften Grade in den x_i. Es sind Kovarianten der Grundkurve (Kombinanten von φ und ψ), und es besteht zwischen ihnen die Relation:

$$\text{(25)}\qquad H^3 - 48 A H f^2 - 64 B f^3 = -27 T^2.$$

Das allgemeinste zu der Grundkurve gehörige Integral (2) geht durch Einführung homogener Variabler $z = x_3 : x_4$ in folgende Form über:

$$\int F(x, y, z)\, \frac{x_3\, dx_4 - x_4\, dx_3}{x_4^2},$$

oder wenn man

$$F(x, y, z) = x_4^2\, \frac{F(x_1, x_2, x_3, x_4)}{\varphi_1 \psi_2 - \varphi_2 \psi_1}$$

setzt, in

$$\int F(x_1, x_2, x_3, x_4)\, \frac{x_3\, dx_4 - x_4\, dx_3}{\varphi_1 \psi_2 - \varphi_2 \psi_1},$$

worin F eine homogene Funktion 0ten Grades ist. Der einfachste Fall ist $F = 1$, und wir betrachten also das Integral erster Gattung:

$$u = \int \frac{x_3\, dx_4 - x_4\, dx_3}{\varphi_1 \psi_2 - \varphi_2 \psi_1}. \tag{26}$$

Nun bilden wir nach dem Multiplikationssatze der Determinanten das Produkt $K(x_3\, dx_4 - x_2\, dx_4)$, also wegen $\varphi = 0$, $\psi = 0$:

$$\begin{vmatrix} \varphi_1, & \varphi_2, & \varphi_3, & \varphi_4 \\ \psi_1, & \psi_2, & \psi_3, & \psi_4 \\ \Phi_1, & \Phi_2, & \Phi_3, & \Phi_4 \\ \Psi_1, & \Psi_2, & \Psi_3, & \Psi_4 \end{vmatrix} \begin{vmatrix} 1, & 0, & 0, & 0 \\ 0, & 1, & 0, & 0 \\ x_1, & x_2, & x_3, & x_4 \\ dx_1, & dx_2, & dx_3, & dx_4 \end{vmatrix} = \begin{vmatrix} \varphi_1, & \varphi_2, & 0, & 0 \\ \psi_1, & \psi_2, & 0, & 0 \\ \Phi_1, & \Phi_2, & \Phi, & d\Phi \\ \Psi_1, & \Psi_2, & \Psi, & d\Psi \end{vmatrix}$$

$$= (\varphi_1 \psi_2 - \varphi_2 \psi_1)(\Phi\, d\Psi - \Psi\, d\Phi),$$

und folglich ergibt sich aus (26) und (23)

$$u = \int \frac{\Phi\, d\Psi - \Psi\, d\Phi}{K} = \int \frac{\Phi\, d\Psi - \Psi\, d\Phi}{\sqrt{f(\Phi, -\Psi)}}. \tag{27}$$

Wendet man hierauf die Transformation des § 5 an, indem man x, y durch $\Phi, -\Psi$ ersetzt, so folgt

$$u = \sqrt{3} \int \frac{f\, dH - H\, df}{\sqrt{-(H^3 - 48\, A f^2 H - 64\, B f^3) f}},$$

und wenn man in § 5, (17) $\mu = 3$, also

$$z = -\frac{3\, H}{4\, f}$$

setzt:

$$u = 3 \int \frac{dz}{\sqrt{4\, z^3 - g_2 z - g_3}},$$

$$g_2 = 12.9\, A, \quad g_3 = -4.27\, B.$$

§ 8. Das Jacobische Transformationsprinzip.

Die Jacobische Transformationstheorie stellt sich im allgemeinen die Aufgabe, ein elliptisches Differential durch ein algebraische Substitution auf ein anderes elliptisches Differentia zurückzuführen. Indem wir hier die Grundlagen dieser Theori auseinandersetzen, bedienen wir uns der Darstellung des elliptischen Differentials in homogenen Variablen [§ 1, (4)]:

(1) $$\frac{x\,dy - y\,dx}{\sqrt{f(x,y)}},$$

und substituieren darin für x, y zwei teilerfremde ganze homogene Funktionen gleichen, aber beliebigen Grades n zweier neuer Variablen ξ, η:

(2) $$x = U(\xi,\eta), \qquad y = V(\xi,\eta).$$

Aus den Gleichungen

$$nU = \xi\frac{\partial U}{\partial \xi} + \eta\frac{\partial U}{\partial \eta}, \qquad dU = d\xi\frac{\partial U}{\partial \xi} + d\eta\frac{\partial U}{\partial \eta},$$

$$nV = \xi\frac{\partial V}{\partial \xi} + \eta\frac{\partial V}{\partial \eta}, \qquad dV = d\xi\frac{\partial V}{\partial \xi} + d\xi\frac{\partial V}{\partial \eta}$$

folgt sodann

(3) $$U\,dV - V\,dU = H(\xi\,d\eta - \eta\,d\xi),$$

wenn H die Funktionaldeterminante

(4) $$H = \frac{1}{n}\left(\frac{\partial U}{\partial \xi}\frac{\partial V}{\partial \eta} - \frac{\partial V}{\partial \xi}\frac{\partial U}{\partial \eta}\right)$$

bedeutet.

Danach geht das elliptische Differential (1) in das folgende über:

(5) $$H\frac{\xi\,d\eta - \eta\,d\xi}{\sqrt{f(U,V)}}.$$

Damit nun dieses Differential wieder die Form eines elliptischen erhält, ist erforderlich, daß von der Funktion $f(U,V)$, deren Grad der $4n$te ist, sich ein quadratischer Faktor T^2 vom Grade $4n-4$ absondern lasse, also, wenn $\varphi(\xi,\eta)$ eine Funktion vierten Grades bedeutet, daß

(6) $$f(U,V) = T^2\varphi(\xi,\eta)$$

werde, wodurch, wenn

(7) $$\frac{T}{H} = M$$

gesetzt wird, das Differential (5) in

$$\frac{1}{M}\frac{\xi d\eta - \eta d\xi}{\sqrt{\varphi(\xi,\eta)}} \tag{8}$$

übergeht. Es läßt sich nun nachweisen, daß, sobald die Bedingung (6) erfüllt ist, H durch T teilbar, und also, da der Grad beider Funktionen derselbe ist, M eine Konstante wird. Diese Konstante heißt der Multiplikator der Transformation.

Bemerken wir nämlich, daß, da $f(x,y)$ keinen quadratischen Faktor enthält, die beiden Funktionen

$$\frac{\partial f}{\partial x}, \quad \frac{\partial f}{\partial y}$$

keinen gemeinschaftlichen Teiler haben, und daß infolgedessen, weil U und V teilerfremd sind, auch

$$\frac{\partial f}{\partial U}, \quad \frac{\partial f}{\partial V}$$

keinen gemeinschaftlichen Teiler (in Beziehung auf ξ, η) haben, so lassen sich zwei Funktionen α, β von ξ, η so bestimmen, daß

$$\alpha\frac{\partial f}{\partial U} + \beta\frac{\partial f}{\partial V}$$

zu einer beliebig gegebenen Funktion T teilerfremd ist. Man kann z. B. α teilerfremd zu T und β durch die in $\frac{\partial f}{\partial U}$ nicht aufgehenden Teiler von T teilbar, dagegen durch die gemeinschaftlichen Teiler von T und $\frac{\partial f}{\partial U}$ unteilbar annehmen. Wenn wir nun die Gleichung (6), die wir als erfüllt voraussetzen, nach ξ, η differentiieren, so folgt:

$$\frac{\partial f}{\partial U}\frac{\partial U}{\partial \xi} + \frac{\partial f}{\partial V}\frac{\partial V}{\partial \xi} = TX,$$
$$\frac{\partial f}{\partial U}\frac{\partial U}{\partial \eta} + \frac{\partial f}{\partial V}\frac{\partial V}{\partial \eta} = TY,$$

und daraus durch Auflösung in bezug auf $\frac{\partial f}{\partial U}$, $\frac{\partial f}{\partial V}$:

$$H\left(\alpha\frac{\partial f}{\partial U} + \beta\frac{\partial f}{\partial V}\right) = TZ,$$

worin X, Y, Z ganze homogene Funktionen von ξ, η sind. Aus der letzten Gleichung aber schließt man, daß H durch T teilbar sein muß.

Demnach ist unser ganzes Problem enthalten in der Gleichung (6), die nichts anderes besagt, als daß die Funktion $4n$ten Grades $f(U,V)$, $2n-2$ quadratische Faktoren enthalten soll. Zur Befriedigung der hieraus folgenden $(2n-2)$ Bedingungen hat man die $2n+2$ in U, V enthaltenen Koeffizienten zur Verfügung, so daß vier von diesen unbestimmt bleiben. Dies war vorauszusehen, da für ξ, η beliebige homogene lineare Funktionen von ξ, η eingeführt werden können. Man kann diese vier überzähligen Konstanten dazu verwenden, um das Differential (8) in eine Normalform zu bringen. Da aber die Bedingungsgleichungen für die Koeffizienten von U, V nicht linear sind, so gibt es für einen gegebenen Transformationsgrad mehrere Transformationen.

Wir werden diesem Transformationsproblem später von einer ganz anderen Seite her wieder begegnen und weit tiefer darauf eingehen müssen. Es soll daher auf die Einzelheiten des algebraischen Problems hier nicht näher eingegangen werden; dagegen wollen wir durch zwei Beispiele das Gesagte veranschaulichen.

§ 9. Die Transformation zweiten Grades.

Wir setzen, um die elliptischen Differentiale in der Normalform zu erhalten:

$$f(x,y) = xy(x-y)(x-\lambda^2 y),$$
$$\varphi(\xi,\eta) = \xi\eta(\xi-\eta)(\xi-\varkappa^2\eta),$$

und es seien U, V vom zweiten Grade.

Die Gleichung (6), § 8, wird jetzt, da T vom zweiten Grade ist

$$(1)\qquad UV(U-V)(U-\lambda^2 V) = (a\xi+b\eta)^2(a'\xi+b'\eta)^2\xi\eta(\xi-\eta)(\xi-\varkappa^2\eta),$$

und es müssen zwei der vier Faktoren zweiten Grades auf der linken Seite dieser Gleichung Quadrate sein. Die große Zahl der hierin liegenden Möglichkeiten wollen wir dadurch noch beschränken, daß wir voraussetzen, η und y sollen gleichzeitig verschwinden, also V durch η teilbar sein. Dies gibt (von einem konstanten Faktor abgesehen) für V die folgenden drei Möglichkeiten:

1. $V=\xi\eta$, 2. $V=\eta(\xi-\eta)$, 3. $V=\eta(\xi-\varkappa^2\eta)$.

Jeder dieser drei Fälle umfaßt nun wieder drei Unterfälle, indem von den drei übrigen Faktoren U, $U-V$, $U-\lambda^2 V$ irgend zwei als Quadrate angenommen werden können. Von diesen letzteren

drei Fällen gehen zwei ineinander über durch Vertauschung von V, λ^2 mit $V:\lambda^2$, $1:\lambda^2$.

Wir wollen zwei für die Folge besonders wichtige unter diesen Transformationen vollständig durchführen.

1. Die Gausssche Transformation.

$$V = \xi\eta, \qquad U = (a\xi + b\eta)^2.$$

Wenn nun noch $U - \lambda^2 V$ ein Quadrat sein soll, so ist

$$\lambda^2 = 4ab$$

zu setzen, und es wird

$$U - \lambda^2 V = (a\xi - b\eta)^2.$$

Da $U - V$ sodann durch $\xi - \eta$ und durch $\xi - \varkappa^2\eta$ teilbar sein muß, so ergeben sich, wenn man $\xi = \eta$, $\xi = \varkappa^2\eta$ setzt, aus $U = V$ die Bedingungen

$$a + b = \pm 1, \qquad a\varkappa^2 + b = \pm\varkappa,$$

woraus, wenn die oberen Zeichen genommen werden,

$$a = \frac{1}{1+\varkappa}, \qquad b = \frac{\varkappa}{1+\varkappa}, \qquad \lambda = \frac{2\sqrt{\varkappa}}{1+\varkappa},$$

$$V = \xi\eta, \qquad U = \left(\frac{\xi + \varkappa\eta}{1+\varkappa}\right)^2, \qquad U - \lambda^2 V = \left(\frac{\xi - \varkappa\eta}{1+\varkappa}\right)^2,$$

$$U - V = \frac{(\xi - \eta)(\xi - \varkappa^2\eta)}{(1+\varkappa)^2},$$

$$T = \frac{\xi^2 - \varkappa^2\eta^2}{(1+\varkappa)^3}, \qquad H = \frac{\xi^2 - \varkappa^2\eta^2}{(1+\varkappa)^2},$$

$$M = \frac{1}{1+\varkappa}.$$

Setzt man also wieder

$$\frac{y}{x} = z, \qquad \frac{\eta}{\xi} = \zeta,$$

so haben wir das Resultat, daß durch die Substitution

$$(2) \qquad z = \frac{(1+\varkappa)^2\zeta}{(1+\varkappa\zeta)^2}, \qquad \lambda^2 = \frac{4\varkappa}{(1+\varkappa)^2}$$

die Transformation

$$(3) \qquad \frac{dz}{\sqrt{z(1-z)(1-\lambda^2 z)}} = \frac{(1+\varkappa)\,d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}$$

geleistet wird.

2. Die Landensche Transformation.

$$V = a\eta(\xi - \eta), \qquad U = \xi(\xi - \varkappa^2\eta).$$

Die Bedingungen, daß $U - V$, $U - \lambda^2 V$ Quadrate sind, lauten

$$4a = (\varkappa^2 + a)^2, \qquad 4a\lambda^2 = (\varkappa^2 + a\lambda^2)^2,$$

woraus

$$\lambda(\varkappa^2 + a) = \varkappa^2 + a\lambda^2,$$

oder durch $\lambda - 1$ dividiert

$$a\lambda = \varkappa^2;$$

dies in eine der obigen Gleichungen eingesetzt, gibt

$$4\lambda = \varkappa^2(1 + \lambda)^2,$$

und durch Auflösung dieser quadratischen Gleichung, wenn $\varkappa' = \sqrt{1 - \varkappa^2}$ gesetzt ist:

$$\lambda = \frac{1 - \varkappa'}{1 + \varkappa'}, \qquad a = (1 + \varkappa')^2,$$

$$U - V = [\xi - (1 + \varkappa')\eta]^2,$$

$$U - \lambda^2 V = [\xi - (1 - \varkappa')\eta]^2,$$

$$H = (1 + \varkappa')^2[\xi - (1 + \varkappa')\eta][\xi - (1 - \varkappa')\eta],$$

$$T = (1 + \varkappa')[(\xi - \eta)^2 - \varkappa'^2\eta^2],$$

$$M = \frac{1}{1 + \varkappa'},$$

also durch die Substitution

$$(4) \qquad z = \frac{(1 + \varkappa')^2\xi(1 - \xi)}{1 - \varkappa^2\xi}, \qquad \lambda = \frac{1 - \varkappa'}{1 + \varkappa'},$$

die Umformung:

$$(5) \qquad \frac{dz}{\sqrt{z(1 - z)(1 - \lambda^2 z)}} = \frac{(1 + \varkappa')d\xi}{\sqrt{\xi(1 - \xi)(1 - \varkappa^2\xi)}}.$$

Wendet man auf die linke Seite dieser Gleichung wieder die Gausssche Transformation an, indem man in den Formeln (2), (3) ξ, $\varkappa$ durch z, λ und z durch eine Variable η ersetzt, so ist, wie aus (2) und (4) folgt, λ in (3) durch $\varkappa$ zu ersetzen, und durch Kombination von (5) und (3) findet man:

$$(6) \qquad \frac{d\eta}{\sqrt{\eta(1 - \eta)(1 - \varkappa^2\eta)}} = \frac{2\,d\xi}{\sqrt{\xi(1 - \xi)(1 - \varkappa^2\xi)}},$$

und die Verbindung von (2) und (4) ergibt zwischen den Variablen η und ξ den Zusammenhang:

$$(7) \qquad \eta = \frac{4\xi(1 - \xi)(1 - \varkappa^2\xi)}{(1 - \varkappa^2\xi^2)^2}.$$

Die Kombination der beiden Transformationen zweiten Grades gibt also die Multiplikation mit 2.

§ 10. Die Transformation dritten Grades.

Als zweites Beispiel betrachten wir die Transformation dritten Grades. Die Gleichung

$$UV(U-V)(U-\lambda^2 V) = T^2 \xi\eta(\xi-\eta)(\xi-\varkappa^2\eta) \tag{1}$$

fordert, daß jeder der vier Faktoren dritten Grades U, V, $U-V$, $U-\lambda^2 V$ durch einen der Linearfaktoren ξ, η, $\xi-\eta$, $\xi-\varkappa^2\eta$ teilbar und daß der Quotient ein Quadrat sei. Wir setzen also

$$U = \xi(a\xi + b\eta)^2, \qquad V = \eta(a'\xi + b'\eta)^2, \tag{2}$$

und verlangen noch, daß

$$\frac{U-V}{\xi-\eta}, \quad \frac{U-\lambda^2 V}{\xi-\varkappa^2\eta} \tag{3}$$

die Quadrate linearer Funktionen werden.

Von den beiden letzten Forderungen folgt die eine aus der anderen, wenn wir U, V so einrichten, daß, von konstanten Faktoren abgesehen, U und V ineinander übergehen durch die Vertauschung von ξ, η mit $\varkappa^2\eta$, ξ. Durch diese Vertauschung geht aber

$$\xi(a\xi + b\eta)^2, \qquad \eta(a'\xi + b'\eta)^2$$

über in

$$\varkappa^2\eta(b\xi + a\varkappa^2\eta)^2, \qquad \xi(b'\xi + a'\varkappa^2\eta)^2,$$

und unsere Forderung ist erfüllt, wenn

$$\varkappa^2 = \frac{bb'}{aa'} \tag{4}$$

ist. Wenn dann

$$\lambda^2 = \varkappa^2\left(\frac{ab}{a'b'}\right)^2 \tag{5}$$

ist, so geht durch diese Vertauschung

$$\frac{U-V}{\xi-\eta} \text{ in } \frac{b'^2}{a^2}\,\frac{U-\lambda^2 V}{\xi-\varkappa^2\eta} \tag{6}$$

über. Nachdem dies festgesetzt, ist nur noch die Bedingung zu erfüllen, daß die erste der beiden Größen (3) das Quadrat einer linearen Funktion wird, die wir mit $(\alpha^2\xi - \beta^2\eta)$ bezeichnen, also:

$$U - V = (\xi-\eta)(\alpha^2\xi - \beta^2\eta)^2 \tag{7}$$

oder

$$U - \xi(\alpha^2\xi - \beta^2\eta)^2 = V - \eta(\alpha^2\xi - \beta^2\eta)^2,$$

und da U durch ξ, V durch η teilbar ist, so muß diese Funktion durch $\xi\eta$ teilbar sein; setzen wir sie $= \xi\eta(m\xi + n\eta)$, so ergibt sich aus (2)

$$(a\xi + b\eta)^2 = (\alpha^2\xi - \beta^2\eta)^2 + \eta(m\xi + n\eta),$$
$$(a'\xi + b'\eta)^2 = (\alpha^2\xi - \beta^2\eta)^2 + \xi(m\xi + n\eta).$$

Die Vergleichung der Koeffizienten ergibt

$$a = \alpha^2, \quad b = -\beta^2 + \frac{m}{2\alpha^2}, \quad b^2 = \beta^4 + n,$$

$$b' = \beta^2, \quad a' = -\alpha^2 + \frac{n}{2\beta^2}, \quad a'^2 = \alpha^4 + m,$$

und aus den beiden letzten Gleichungen jeder Reihe:

$$m^2 = 4\alpha^2(n\alpha^2 + m\beta^2),$$
$$n^2 = 4\beta^2(n\alpha^2 + m\beta^2).$$

Wenn man also

$$m = h\alpha, \qquad n = h\beta$$

setzt, so wird

$$h = 4\alpha\beta\,(\alpha + \beta).$$

Hiernach lassen sich a, b, a', b' durch die beiden Größen α, β ausdrücken in der Weise:

(8) $$a = \alpha^2, \quad b = \beta^2 + 2\alpha\beta,$$
$$a' = \alpha^2 + 2\alpha\beta, \quad b' = \beta^2,$$

und danach aus (4), (5)

(9) $$\varkappa^2 = \frac{\beta^3}{\alpha^3}\,\frac{\beta + 2\alpha}{\alpha + 2\beta}, \quad \frac{\lambda}{\varkappa} = \frac{\alpha}{\beta}\,\frac{\beta + 2\alpha}{\alpha + 2\beta},$$

oder durch Multiplikation und Division dieser beiden Gleichungen:

(10) $$\sqrt{\lambda\varkappa} = \frac{\beta}{\alpha}\,\frac{\beta + 2\alpha}{\alpha + 2\beta}, \quad \frac{\varkappa^3}{\lambda} = \frac{\beta^4}{\alpha^4}.$$

Durch Elimination von $\beta:\alpha$ erhält man eine Gleichung zwischen $\varkappa$, λ, die man die Modulargleichung nennt, deren Grad die Anzahl der verschiedenen Transformationen dritten Grades angibt. Sie nimmt die einfachste Gestalt an, wenn man setzt:

(11) $$\sqrt[4]{\varkappa} = u, \quad \sqrt[4]{\lambda} = v.$$

Dann werden die Gleichungen (10)

$$u^2v^2 = \frac{\beta}{\alpha}\,\frac{\beta + 2\alpha}{\alpha + 2\beta}, \quad \frac{u^3}{v} = \frac{\beta}{\alpha},$$

also durch Einsetzen des Wertes von $\beta:\alpha$ in die erste Gleichung und Beseitigung des Faktors u^2:

(12) $$v^4 - u^4 + 2u^3v^3 - 2uv = 0,$$

eine Gleichung vom vierten Grade.

Man erhält ferner [ohne weitläufige Rechnung durch Vergleichung der Koeffizienten der höchsten Potenz von ξ in (1)]

$$T = \frac{a}{b'}(a\xi + b\eta)\,(a'\xi + b'\xi)\,(\alpha^2\xi - \beta^2\eta)\,(\beta^2\xi - \varkappa^2\alpha^2\eta),$$

$$H = \frac{1}{3}\left(\frac{\partial U}{\partial \xi}\frac{\partial V}{\partial \eta} - \frac{\partial V}{\partial \xi}\frac{\partial U}{\partial \eta}\right) = \frac{a'}{a}T,$$

woraus man leicht nach (8) findet:

$$M = \frac{a}{a'} = \frac{\alpha}{\alpha + 2\beta} = \frac{v}{v + 2u^3}. \tag{13}$$

Setzt man den hieraus sich ergebenden Ausdruck

$$v = \frac{2u^3 M}{1 - M}$$

in die Gleichung (12) ein, so ergibt sich für M eine Gleichung vierten Grades, die Multiplikatorgleichung, die die Modulargleichung ersetzen kann. Man erhält aber diese Gleichung einfacher auf folgendem Wege. Nach (13) ist

$$\frac{1}{M} - 1 = 2\frac{\beta}{\alpha}, \quad \frac{1}{M} + 3 = \frac{2(\beta + 2\alpha)}{\alpha},$$

also nach (9):

$$\left(\frac{1}{M} - 1\right)^3\left(\frac{1}{M} + 3\right) = 16\varkappa^2\frac{\alpha + 2\beta}{\alpha},$$

und folglich nach (13)

$$\frac{16\varkappa^2}{M} = \left(\frac{1}{M} - 1\right)^3\left(\frac{1}{M} + 3\right),$$

oder geordnet

$$\frac{1}{M^4} - \frac{6}{M^2} + \frac{8(1 - 2\varkappa^2)}{M} - 3 = 0. \tag{14}$$

Drücken wir also unsere Formeln durch u, v aus, so ist das Ergebnis dieser Betrachtung das folgende:

Durch die Substitution

$$z = -\frac{\zeta[(v^2 + 2vu^3) + u^6\zeta]^2}{[v^2 + (u^6 + 2vu^3)\zeta]^2}$$

wird die Transformation bewirkt

$$\frac{dz}{\sqrt{z(1 - z)(1 - v^8 z)}} = \frac{v + 2u^3}{v}\frac{d\zeta}{\sqrt{\zeta(1 - \zeta)(1 - u^8\zeta)}},$$

falls zwischen u, v die Modulargleichung (12) besteht.

Zu einem gegebenen u ergibt die Modulargleichung vier Werte von v, also vier verschiedene Transformationen dritten Grades.

§ 11. Die drei Gattungen elliptischer Integrale.

Es sei jetzt

(1) $$f(x) = a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$$

eine ganze Funktion dritten oder vierten Grades, und

(2) $$\Omega(x) = \int \frac{\Phi(x)\, dx}{\sqrt{f(x)}} = \int R(x)\, dx,$$

wenn zur Abkürzung

(3) $$R(x) = \frac{\Phi(x)}{\sqrt{f(x)}}$$

gesetzt ist, ein elliptisches Integral. Es bedeutet darin x eine unbeschränkt veränderliche (auch komplexe) Größe, und $\sqrt{f(x)}$ hat für jeden Wert von x, für den $f(x)$ nicht verschwindet, zwei entgegengesetzte Werte. Wir verstehen unter einem Punkt nicht einen Wert von x allein, sondern ein zusammengehöriges Wertepaar von x und $\sqrt{f(x)}$, also einen Wert von x mit einem bestimmten Vorzeichen von $\sqrt{f(x)}$. Ist daher x_0 irgend ein Wert von x, so gibt es zwei Punkte x_0, wenn $f(x_0)$ von Null verschieden ist, aber nur einen, wenn $f(x_0) = 0$ ist. Für $x = \infty$ bestimmen wir die Punkte nach dem Vorzeichen von $\sqrt{f(x)} : x^2$, und wir haben also zwei Punkte $x = \infty$, wenn $f(x)$ vom vierten, und nur einen, wenn $f(x)$ vom dritten Grade ist.

Nach bekannten Sätzen der Funktionentheorie gibt es, wenn $f(x_0)$ von Null verschieden ist, eine in einem gewissen Bereich konvergente Entwickelung nach dem Taylorschen Lehrsatz:

(4) $$R(x) = A_m(x-x_0)^m + A_{m+1}(x-x_0)^{m+1} + A_{m+2}(x-x_0)^{m+2} + \cdots,$$

worin m eine positive oder negative ganze Zahl oder auch Null ist, während $A_m, A_{m+1}, A_{m+2}, \ldots$ Konstanten bedeuten, von denen A_m nicht verschwindet. Dies ist eine Entwickelung nach steigenden Potenzen. Ergänzend tritt hinzu, falls $f(x)$ vom vierten (nicht vom dritten) Grade ist, die Entwickelung nach fallenden Potenzen

(5) $$R(x) = C_m x^{-m-2} + C_{m+1} x^{-m-3} + C_{m+2} x^{-m-4} + \cdots,$$

von der wir sagen, daß sie in der Umgebung eines unendlich fernen Punktes gilt.

Wenn aber $f(x_0)$ verschwindet, so erhält die Entwickelung von $R(x)$ die Form:

$$(6)\qquad R(x) = A_m(x-x_0)^{m-1/2} + A_{m+1}(x-x_0)^{m-1/2+1} + A_{m+2}(x-x_0)^{m-1/2+2} + \cdots,$$

und wenn $f(x)$ vom dritten Grade ist, so gilt in der Umgebung des unendlich fernen Punktes die Entwickelung

$$(7)\qquad R(x) = C_m x^{-m-3/2} + C_{m+1} x^{-m-5/2} + C_{m+2} x^{-m-7/2} + \cdots$$

Aus den Entwickelungen (4) bis (7) können wir die Entwickelungen von Ω ableiten, wobei eine additive Konstante unbestimmt bleibt.

Die Entwickelung von Ω ist dann ebenfalls eine Potenzreihe, wozu, wenn m negativ ist, in den Fällen (4) oder (5) noch ein Glied $A_{-1}\log(x-x_0)$, $C_{-1}\log x$ tritt.

Wir nennen nun x_0 einen Punkt erster Gattung von Ω, wenn m in diesen Entwickelungen nicht negativ ist.

Dann ist Ω im Punkte x_0 endlich (auch im Falle $x_0 = \infty$).

Der Punkt x_0 heißt ein Punkt zweiter Gattung von Ω, wenn in den Entwickelungen (4), (5) m negativ und $A_{-1} = 0$, $C_{-1} = 0$ ist, und in dem Falle der Entwickelung (6), (7) mit negativem m.

Endlich heißt x_0 ein Punkt dritter Gattung, wenn in den Entwickelungen (4) oder (5) A_{-1} oder C_{-1} von Null verschieden ist, wenn also in der Entwickelung von Ω ein logarithmisches Glied vorkommt.

Die Nullpunkte von $f(x)$ können bei dem Integral (2) nicht von der dritten Gattung sein; sie können aber von der dritten Gattung werden, wenn wir das elliptische Integral in der allgemeinen Form $\int \Phi(x, \sqrt{f(x)})\,dx$ betrachten.

Das Integral Ω heißt ein Integral erster Gattung, wenn es nur Punkte erster Gattung hat. Ein solches Integral hat dann für alle endlichen und unendlichen Werte von x einen endlichen Wert.

Ω heißt ein Integral zweiter Gattung, wenn es nur Punkte erster und zweiter Gattung hat, und

Ω heißt ein Integral dritter Gattung, wenn es neben Punkten erster und zweiter Gattung auch Punkte dritter Gattung hat.

§ 12. Darstellung der elliptischen Integrale durch die einfachsten Grundintegrale.

Um das Integral $\Omega(x)$ durch Integrale von möglichst einfachem Typus darzustellen, zerlegen wir die rationale Funktion $\Phi(x)$ in eine ganze Funktion und in eine Summe von Partialbrüchen, d. h. wir stellen $\Phi(x)$ dar als eine Summe von Ausdrücken der Form

$$x^n, \quad \frac{1}{(x-\alpha)^n}$$

mit konstanten Koeffizienten, worin n eine ganze positive Zahl (auch Null) und α einen konstanten Wert bedeutet, für den $\Phi(x)$ unendlich wird.

Setzen wir dann für positive und für negative oder verschwindende n

$$(1) \qquad S_n(\alpha) = \int \frac{(x-\alpha)^n dx}{\sqrt{f(x)}},$$

so wird $\Omega(x)$ eine Summe der Form

$$\Omega(x) = \sum M S_n(\alpha),$$

wo sich die Summe auf mehrere verschiedene Werte von n und von α erstrecken kann und die M Konstanten sind.

Die Funktionen S_n lassen sich durch Vermittelung algebraischer Funktionen auf eine geringe Anzahl zurückführen. Zu dem Ende bilden wir

$$d(x-\alpha)^n \sqrt{f(x)} = \frac{n(x-\alpha)^{n-1} f(x) + (x-\alpha)^n \frac{1}{2} f'(x)}{\sqrt{f(x)}},$$

und wenn wir darin setzen

$$f(x) = f(\alpha) + (x-\alpha) f'(\alpha) + \frac{(x-\alpha)^2}{2} f''(\alpha) + \frac{(x-\alpha)^3}{6} f'''(\alpha) + \frac{(x-\alpha)^4}{24} f''''(\alpha),$$

$$f'(x) = f'(\alpha) + (x-\alpha) f''(\alpha) + \frac{(x-\alpha)^2}{2} f'''(\alpha) + \frac{(x-\alpha)^3}{6} f''''(\alpha),$$

so folgt

$$(2) \qquad \begin{aligned} (x-\alpha)^n \sqrt{f(x)} = {} & n f(\alpha) S_{n-1} + \left(n + \frac{1}{2}\right) f'(\alpha) S_n \\ & + \frac{n+1}{2} f''(\alpha) S_{n+1} + \left(\frac{n}{6} + \frac{1}{4}\right) f'''(\alpha) S_{n+2} \\ & + \left(\frac{n}{24} + \frac{1}{12}\right) f''''(\alpha) S_{n+3}. \end{aligned}$$

Wir unterscheiden vier Fälle:

1. $f''''(\alpha)$ und $f(\alpha)$ nicht $= 0$ [d. h. $f(x)$ vom vierten Grade und α keine Wurzel von $f(x)$].

In diesem Falle läßt sich durch die Formel (2) für $n = 0$ S_3 durch S_0, S_1, S_2 ausdrücken, und daher S_n für jedes positive n durch S_0, S_1, S_2. Setzt man aber $n = -1, -2, \ldots$, so erhält man S_{-2}, S_{-3}, ... ausgedrückt durch S_{-1}, S_0, S_1, S_2. Also bleiben in diesem Falle die vier Grundintegrale

$$S_{-1}, \quad S_0, \quad S_1, \quad S_2.$$

2. $f''''(\alpha)$ nicht $= 0$, $f(\alpha) = 0$. In diesem Falle kann man noch S_{-1} durch S_0, S_1, S_2 ausdrücken und erhält als Grundintegrale

$$S_0, \quad S_1, \quad S_2.$$

3. $f''''(\alpha) = 0$, $f(\alpha)$ nicht $= 0$. Hier sind die Grundintegrale

$$S_{-1}, \quad S_0, \quad S_1.$$

4. $f''''(\alpha) = 0$, $f(\alpha) = 0$. Hier sind die Grundintegrale

$$S_0, \quad S_1.$$

Das Resultat hiervon ist also:

I. Ist $f(x)$ vom vierten Grade ($a_0 = 1$), so lassen sich alle Integrale $\Omega(x)$ ausdrücken durch Integrale der Form

$$S_0 = \int \frac{dx}{\sqrt{f(x)}}, \quad S_1 = \int \frac{x\,dx}{\sqrt{f(x)}}, \quad S_2 = \int \frac{x^2\,dx}{\sqrt{f(x)}},$$
$$S_{-1} = \int \frac{dx}{(x-\alpha)\sqrt{f(x)}},$$

worin S_{-1} noch von dem Parameter α abhängig ist.

II. Ist aber $f(x)$ vom dritten Grade, so genügen die drei Integrale

$$S_0 = \int \frac{dx}{\sqrt{f(x)}}, \quad S_1 = \int \frac{x\,dx}{\sqrt{f(x)}}, \quad S_{-1} = \int \frac{dx}{(x-\alpha)\sqrt{f(x)}}.$$

In beiden Fällen ist S_0 von der **ersten Gattung**. Ist $f(x)$ vom dritten Grade, so ist S_1 von der zweiten und S_{-1} von der dritten Gattung. Ist dagegen $f(x)$ vom vierten Grade, so sind S_1, S_2 und S_{-1} von der dritten Gattung. Man kann aber aus S_1 und S_2 ein Integral zweiter Gattung zusammensetzen. Denn es ist

$$\frac{1}{\sqrt{f(x)}} = (x^4 + a_1 x^3 + a_2 x^2 + a_3 x^2 + a_4)^{-1/2}$$
$$= x^{-2} - \frac{a_1}{2} x^{-3} + \cdots,$$

und in der Entwickelung von $\left(x^2 + \frac{a_1}{2} x\right) : \sqrt{f(x)}$ nach fallenden Potenzen kommt kein Glied mit x^{-1} vor. Folglich ist $S_2 + \frac{a_2}{2} S_1$ ein Integral zweiter Gattung.

Durch Vermittelung einer logarithmischen Funktion kann man aber auch noch die vier Integrale des Falles I auf drei reduzieren. Zu dem Ende bringe man $f(x)$ auf die Form

$$x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = P^2 + a x + b,$$

worin $P = x^2 + p x + q$ eine quadratische Funktion und a und b Konstanten sind. Es ergibt sich:

$$p = \frac{a_1}{2}, \qquad q = \frac{a_2}{2} - \frac{a_1^2}{8},$$
$$a = a_3 - \frac{a_1 a_2}{2} + \frac{a_1^3}{8}, \qquad b = a_4 - \left(\frac{a_2}{2} - \frac{a_1^2}{8}\right)^2.$$

Nun ist:

$$(3) \qquad d \log \frac{\sqrt{f} - P}{\sqrt{f} + P} = \frac{f'(x) P - 2 f(x) P'(x)}{f - P^2} \frac{dx}{\sqrt{f(x)}},$$
$$f - P^2 = a x + b,$$
$$f'(x) = 2 P P' + a$$

und folglich

$$f'(x) P - 2 f(x) P'(x) = a(P - 2 x P') - 2 b P' = Q$$

eine quadratische Funktion von x, und demnach ergibt sich aus (3)

$$(4) \qquad \log \frac{\sqrt{f} - P}{\sqrt{f} + P} = \int \frac{Q}{a x + b} \frac{dx}{\sqrt{f(x)}}.$$

Die rechte Seite ist aber eine lineare Funktion von S_0, S_1 und S_{-1} (für $\alpha = -b/a$). In dem besonderen Falle, wo $a = 0$ ist, wird Q vom ersten Grade, und man kann eine lineare Verbindung von S_0 und S_{-1} durch eine logarithmische Funktion ausdrücken.

Nehmen wir a_1 und $a_3 = 0$ an, worauf wir den allgemeinen Fall nach § 4 durch lineare Transformation zurückführen können, so erhalten wir als die Grundintegrale

$$S_0 = \int \frac{dx}{\sqrt{f(x)}}, \quad S_2 = \int \frac{x^2\,dx}{\sqrt{f(x)}}, \quad S_{-1} = \int \frac{dx}{(x-\alpha)\sqrt{f(x)}},$$

während $S_1 = \int \frac{x\,dx}{\sqrt{f(x)}}$ durch die Substitution $x^2 = y$ auf das nicht elliptische Integral

$$\frac{1}{2}\int \frac{dy}{\sqrt{y^2 + a_2 y + a_4}}$$

zurückgeführt wird. Hier ist S_0 von der ersten, S_2 von der zweiten, S_{-1} von der dritten Gattung. Für die Legendresche Normalform setzen wir $f(x) = (1 - x^2)(1 - \varkappa^2 x^2)$ und nehmen als Normalintegral der zweiten Gattung nicht S_2 selbst, sondern $S_0 - \varkappa^2 S_2$. Dadurch ergeben sich die Normalintegrale der drei Gattungen:

$$\int \frac{dx}{\sqrt{(1-x^2)(1-\varkappa^2 x^2)}}, \int \sqrt{\frac{1-\varkappa^2 x^2}{1-x^2}}\,dx, \int \frac{dx}{(x-\alpha)\sqrt{(1-x^2)(1-\varkappa^2 x^2)}}$$

und wenn man $x = \sin\varphi$ setzt:

$$\int \frac{d\varphi}{\sqrt{1-\varkappa^2 \sin^2\varphi}}, \quad \int \sqrt{1-\varkappa^2\sin^2\varphi}\,d\varphi, \quad \int \frac{d\varphi}{(\sin\varphi - \alpha)\sqrt{1-\varkappa^2\sin^2\varphi}}.$$

Dasselbe erhält man, wenn man das elliptische Differential in der Normalform

$$\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}}$$

annimmt und nach dem Falle II verfährt.

§ 13. Das Additionstheorem.

Das von Euler entdeckte Additionstheorem der elliptischen Integrale besteht in dem Satze, der für die ganze weitere Theorie von fundamentaler Bedeutung ist, daß, wenn von den drei Wertpaaren

$$x_1, \sqrt{f(x_1)}; \quad x_2, \sqrt{f(x_2)}; \quad x_3, \sqrt{f(x_3)}$$

zwei als gegeben vorausgesetzt werden, man auf algebraischem Wege das dritte so bestimmen kann, daß die Differentialgleichung

$$(1) \qquad \frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} + \frac{dx_3}{\sqrt{f(x_3)}} = 0$$

befriedigt ist. Darin ist $f(x)$ eine gegebene Funktion vom dritten oder vierten Grade. Es ist dies ein spezieller Fall des großen

Abelschen Theorems und soll auch in dieser Weise hier aufgefaßt und abgeleitet werden [1]). Dem Beweise schicken wir folgenden elementaren algebraischen Satz voraus:

Ist $F(x)$ eine ganze rationale Funktion $n$ten Grades ohne mehrfache Faktoren, $F'(x)$ ihre Derivierte, sind ferner $x_1, x_2, \ldots, x_n$ die Wurzeln der Gleichung $F(x) = 0$ und $\varphi(x)$ eine ganze Funktion von x, deren Grad höchstens $= n - 2$, so ist

$$\frac{\varphi(x_1)}{F'(x_1)} + \frac{\varphi(x_2)}{F'(x_2)} + \cdots \frac{\varphi(x_n)}{F'(x_n)} = 0. \tag{2}$$

Der Beweis dieses Satzes ergibt sich unmittelbar aus der Zerlegung des rationalen Bruches

$$\frac{x\,\varphi(x)}{F(x)}$$

in Partialbrüche

$$\frac{x_1\,\varphi(x_1)}{F'(x_1)(x - x_1)} + \frac{x_2\,\varphi(x_2)}{F'(x_2)(x - x_2)} + \cdots + \frac{x_n\,\varphi(x_n)}{F'(x_n)(x - x_n)},$$

wenn darin $x = 0$ gesetzt wird [Bd. I, § 15 (9)].

Es sollen nun P, Q ganze Funktionen von x von den Graden m und $m - 2$ bedeuten, und wir fragen nach den Werten von x, $\sqrt{f(x)}$, für die die Funktion

$$P + Q\sqrt{f(x)} \tag{3}$$

verschwindet. Solcher Wertpaare (Punkte) gibt es $2m$, und zwar findet man die Werte von x als Wurzeln der Gleichung $2m$ten Grades:

$$F(x) = P^2 - Q^2 f(x) = 0, \tag{4}$$

und die zugehörigen Werte von $\sqrt{f(x)}$ aus

$$P + Q\sqrt{f(x)} = 0. \tag{5}$$

Wir nehmen nun an, die Koeffizienten in den Funktionen P, Q seien veränderlich, entweder unabhängige Veränderliche oder in irgend einer Weise von anderen Veränderlichen abhängig.

[1]) Dieses weitumfassende Theorem findet sich in großartiger Einfachheit abgeleitet in einem kaum zwei Seiten umfassenden Aufsatze im vierten Bande von Crelles Journal „Démonstration d'une propriété générale d'une certaine classe de fonctions transcendentes"; Oeuvres complètes de N. H. Abel. Nouvelle édition, T. I, p. 515. Ausführliche Darstellung und Anwendungen in der nachgelassenen großen Abhandlung: „Mémoire sur une propriété générale d'une classe très étendue de fonctions transcendentes".

Es werden dann auch die durch (4), (5) bestimmten Werte x und $\sqrt{f(x)}$ Funktionen dieser Veränderlichen, und (5) läßt sich differentiieren.

Bezeichnen wir mit δ die Differentiation nach den in den Koeffizienten von P, Q vorkommenden Veränderlichen, wobei x als konstant gilt, mit dx das entsprechende Differential von x, wenn x durch (4) oder (5) als Funktion dieser Koeffizienten bestimmt ist, so ergibt die Differentiation von (4)

$$2P\delta P - 2Q\delta Q f(x) + F'(x)\,dx = 0,$$

woraus mit Benutzung von (5):

$$(6)\qquad \frac{Q\delta P - P\delta Q}{F'(x)} = \frac{dx}{2\sqrt{f(x)}},$$

und da der Zähler auf der linken Seite vom Grade $2m - 2$, $F(x)$ vom Grade $2m$ ist, so läßt sich die Formel (2) anwenden, und es folgt

$$(7)\qquad \sum \frac{dx}{\sqrt{f(x)}} = 0,$$

wenn die Summe auf sämtliche Wurzeln der Gleichung (5) erstreckt ist.

Wir wenden dieses Theorem auf den einfachsten Fall, nämlich $m = 2$, an und erhalten dann folgenden Satz:

Wenn

$$(8)\qquad x_1,\ \sqrt{f(x_1)};\quad x_2,\ \sqrt{f(x_2)};\quad x_3,\ \sqrt{f(x_3)};\quad x_4,\ \sqrt{f(x_4)}$$

vier Wertepaare sind, für die irgend eine Funktion der Form

$$(9)\qquad a + bx + cx^2 + \sqrt{f(x)}$$

verschwindet, so sind diese Wertepaare nicht gänzlich voneinander unabhängig, sondern es besteht zwischen ihnen die Differentialgleichung

$$(10)\qquad \frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} + \frac{dx_3}{\sqrt{f(x_3)}} + \frac{dx_4}{\sqrt{f(x_4)}} = 0.$$

Die Abhängigkeit dieser vier Wertepaare, also eine Integration der Differentialgleichung (10), kann aber auch in algebraischer Weise ausgedrückt werden, indem man die Funktion (9) für $x = x_1, x_2, x_3, x_4$ gleich Null setzt und dann a, b, c eliminiert. Man erhält so die Determinantengleichung:

$$(11)\qquad \begin{vmatrix} 1, & x_1, & x_1^2, & \sqrt{f(x_1)} \\ 1, & x_2, & x_2^2, & \sqrt{f(x_2)} \\ 1, & x_3, & x_3^2, & \sqrt{f(x_3)} \\ 1, & x_4, & x_4^2, & \sqrt{f(x_4)} \end{vmatrix} = 0.$$

Aus dieser Gleichung kann man x_1 und $\sqrt{f(x_1)}$ rational durch x_2, $\sqrt{f(x_2)}$; x_3, $\sqrt{f(x_3)}$; x_4, $\sqrt{f(x_4)}$ ausdrücken; denn x_1 ist die Wurzel einer biquadratischen Gleichung, deren drei andere Wurzeln x_2, x_3, x_4 sind, und deren Koeffizienten rational von x_2, $\sqrt{f(x_2)}$; x_3, $\sqrt{f(x_3)}$; x_4, $\sqrt{f(x_4)}$ abhängen, und $\sqrt{f(x_1)}$ ist mittels (11) rational durch x_1 darstellbar. Setzt man x_4 einer beliebigen Konstanten gleich, so geht die Differentialgleichung (10) in (1) über und (11) ergibt ihr Integral.

Wir wenden dies Theorem zunächst auf die Normalform an und setzen

$$f(x) = x(1-x)(1-\varkappa^2 x).$$

Nehmen wir in (11) $x_4 = 0$ an, so reduziert sich diese Gleichung durch Division mit $\sqrt{x_1 x_2 x_3}$ auf:

$$(12)\qquad \begin{vmatrix} \sqrt{x_1}, & x_1\sqrt{x_1}, & \sqrt{(1-x_1)(1-\varkappa^2 x_1)} \\ \sqrt{x_2}, & x_2\sqrt{x_2}, & \sqrt{(1-x_2)(1-\varkappa^2 x_2)} \\ \sqrt{x_3}, & x_3\sqrt{x_3}, & \sqrt{(1-x_3)(1-\varkappa^2 x_3)} \end{vmatrix} = 0,$$

oder wenn wir die Determinante nach den Elementen der ersten Zeile entwickeln:

$$(13)\qquad \sqrt{x_1}(a + b x_1) + c\sqrt{(1-x_1)(1-\varkappa^2 x_1)} = 0,$$

worin zur Abkürzung gesetzt ist:

$$(14)\qquad \begin{aligned} a &= x_2\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} - x_3\sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}, \\ b &= -\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} + \sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}, \\ c &= -(x_2 - x_3)\sqrt{x_2}\sqrt{x_3}. \end{aligned}$$

Wenn wir (13) rational machen, so erhalten wir die kubische Gleichung:

$$x(a + b x)^2 - c^2(1-x)(1-\varkappa^2 x) = 0,$$

deren drei Wurzeln x_1, x_2, x_3 sind. Es ist demnach identisch

$$(15)\qquad b^2(x-x_1)(x-x_2)(x-x_3) = x(a+bx)^2 - c^2(1-x)(1-\varkappa^2 x),$$

und indem wir in dieser identischen Gleichung $x = 0, 1, 1:\varkappa^2$ setzen, so folgt:

$$\begin{aligned}
&\sqrt{x_1 x_2 x_3} = -\frac{c}{b} \\
(16)\qquad &\sqrt{(1-x_1)(1-x_2)(1-x_3)} = \frac{b+a}{b} \\
&\sqrt{(1-\varkappa^2 x_1)(1-\varkappa^2 x_2)(1-\varkappa^2 x_3)} = \frac{b+\varkappa^2 a}{b}.
\end{aligned}$$

Zur Bestimmung der Vorzeichen in diesen Gleichungen erhalten wir noch aus (13), wenn wir x_1 durch x_2 und x_3 ersetzen und die Ergebnisse multiplizieren:

$$x_1 x_2 x_3 (a + b x_1)(a + b x_2)(a + b x_3) = -c^3 \sqrt{f(x_1)}\sqrt{f(x_2)}\sqrt{f(x_3)}$$

und (15) ergibt für $x = -a:b$

$$(a + b x_1)(a + b x_2)(a + b x_3) = \frac{c^2}{b}(b+a)(b+\varkappa^2 a).$$

Benutzt man noch das Quadrat der ersten Gleichung (16), so folgt hieraus

$$\sqrt{f(x_1)}\sqrt{f(x_2)}\sqrt{f(x_3)} = -\frac{c}{b^3}(b+a)(b+\varkappa^2 a).$$

Dasselbe Resultat ergibt aber die Multiplikation der drei Gleichungen (16), und die Vorzeichen sind also in diesen Formeln so gewählt, daß das Produkt der linken Seiten den durch die Differentialgleichung (1) geforderten Wert von $\sqrt{f(x_1)}$ ergibt. Eine weitere Bestimmung der Vorzeichen ist in (16) der Natur der Sache nach nicht möglich, und diese Gleichungen dienen zur eindeutigen Definition von $\sqrt{x_1}$, $\sqrt{1-x_1}$, $\sqrt{1-\varkappa^2 x_1}$, wenn die $\sqrt{x_2}$, $\sqrt{1-x_2}$, $\sqrt{1-\varkappa^2 x_2}$, $\sqrt{x_3}$, $\sqrt{1-x_3}$, $\sqrt{1-\varkappa^2 x_3}$ als gegeben vorausgesetzt werden.

Um die Gleichungen (16) in die gebräuchliche Form zu bringen, machen wir zunächst in (14) den Zähler von b rational und erhalten

$$b = \frac{(x_2 - x_3)(1 - \varkappa^2 x_2 x_3)}{\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} + \sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}},$$

ferner nach (14):

$$b + a =$$
$$-\sqrt{(1-x_2)(1-x_3)}\,\{\sqrt{x_2(1-x_2)}\sqrt{1-\varkappa^2 x_3} - \sqrt{x_3(1-x_3)}\sqrt{1-\varkappa^2 x_2}\}$$
$$b + \varkappa^2 a =$$
$$-\sqrt{(1-\varkappa^2 x_2)(1-\varkappa^2 x_3)}\,\{\sqrt{x_2(1-\varkappa^2 x_2)}\sqrt{1-x_3} - \sqrt{x_3(1-\varkappa^2 x_3)}\sqrt{1-x_2}\},$$

wodurch die Gleichungen (16) leicht in die Form gebracht werden:

$$\sqrt{x_1} = -\frac{\sqrt{x_2}\sqrt{(1-x_3)(1-\varkappa^2 x_3)} + \sqrt{x_3}\sqrt{(1-x_2)(1-\varkappa^2 x_2)}}{1-\varkappa^2 x_2 x_3},$$

$$(17)\quad \sqrt{1-x_1} = \frac{\sqrt{1-x_2}\sqrt{1-x_3} - \sqrt{x_2 x_3}\sqrt{(1-\varkappa^2 x_2)(1-\varkappa^2 x_3)}}{1-\varkappa^2 x_2 x_3},$$

$$\sqrt{1-\varkappa^2 x_1} = \frac{\sqrt{1-\varkappa^2 x_2}\sqrt{1-\varkappa^2 x_3} - \varkappa^2\sqrt{x_2 x_3}\sqrt{(1-x_2)(1-x_3)}}{1-\varkappa^2 x_2 x_3},$$

und unsere Betrachtung lehrt, daß, wenn x_1 und die Wurzeln $\sqrt{x_1}$, $\sqrt{1-x_2}$, $\sqrt{1-\varkappa^2 x_1}$ durch diese Gleichungen als Funktionen von x_2, x_3 bestimmt werden, die Differentialgleichung (1) identisch befriedigt ist.

Um auch für die Weierstrasssche Normalform das Additionstheorem in möglichst einfacher Gestalt zu erhalten, setze man

$$f(x) = 4x^3 - g_2 x - g_3,$$

und lasse in der Gleichung (11) (nach Division mit x_4^2) x_4 unendlich groß werden. Es ergibt sich alsdann das Integral der Differentialgleichung (1)

$$\frac{dx_1}{\sqrt{f(x_1)}} + \frac{dx_2}{\sqrt{f(x_2)}} + \frac{dx_3}{\sqrt{f(x_3)}} = 0$$

in der Form

$$(18)\qquad \begin{vmatrix} 1, & x_1, & \sqrt{f(x_1)} \\ 1, & x_2, & \sqrt{f(x_2)} \\ 1, & x_3, & \sqrt{f(x_3)} \end{vmatrix} = 0,$$

oder

$$(19)\qquad a + b x_1 + c\sqrt{f(x_1)} = 0,$$

wenn

$$(20)\qquad \begin{aligned} a &= x_2\sqrt{f(x_3)} - x_3\sqrt{f(x_2)} \\ b &= \sqrt{f(x_2)} - \sqrt{f(x_3)} \\ c &= x_3 - x_2. \end{aligned}$$

Es werden dann x_1, x_2, x_3 die Wurzeln der kubischen Gleichung

$$(a + bx)^2 - c^2 f(x) = 0,$$

und wenn man hierin den Koeffizienten von x^2, geteilt durch den von x^3 gleich der negativen Summe der Wurzeln setzt, so erhält man

$$(21) \qquad x_1 + x_2 + x_3 = \frac{1}{4}\left(\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3}\right)^2,$$

und aus (19)

$$(22) \quad \sqrt{f(x_1)} = \frac{1}{4}\left(\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3}\right)^3 - (x_2 + x_3)\,\frac{\sqrt{f(x_2)} - \sqrt{f(x_3)}}{x_2 - x_3} - \frac{x_3\sqrt{f(x_2)} - x_2\sqrt{f(x_3)}}{x_2 - x_3}.$$

§ 14. Ursprung der elliptischen Funktionen.

Wenn in dem elliptischen Differential erster Gattung in der Legendreschen Normalform

$$\frac{1}{2}\,\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}}$$

die Substitution

$$(1) \qquad z = \sin^2\varphi$$

gemacht und sodann die Integration von $\varphi = 0$ an ausgeführt wird, so entsteht das elliptische Integral erster Gattung

$$(2) \qquad \int_0^{\varphi} \frac{d\varphi}{\sqrt{1 - \varkappa^2 \sin^2\varphi}} = u.$$

Jacobi nennt die obere Grenze φ dieses Integrals seine Amplitude und schreibt

$$(3) \qquad \varphi = \operatorname{am} u.$$

Die trigonometrischen Funktionen dieses Bogens

$$(4) \qquad \sin\varphi,\ \cos\varphi,\ \sqrt{1 - \varkappa^2\sin^2\varphi} = \Delta\varphi$$

sind es nun, die, als Funktionen von u betrachtet, elliptische Funktionen genannt und von Jacobi mit

$$\operatorname{sinam} u, \quad \operatorname{cosam} u, \quad \Delta\operatorname{am} u,$$

oder, nach Gudermann, kürzer mit

$$(5) \qquad \operatorname{sn} u, \quad \operatorname{cn} u, \quad \operatorname{dn} u$$

bezeichnet werden. Diese Funktionen hängen von den zwei Argumenten u und $\varkappa^2$ ab, und wenn eine genauere Bezeichnung notwendig ist, wird dafür auch

$$\operatorname{sn}(u, \varkappa^2), \quad \operatorname{cn}(u, \varkappa^2), \quad \operatorname{dn}(u, \varkappa^2)$$

gesetzt.

Wenn in der Formel (1) φ in $-\varphi$ verwandelt wird, so geht u in $-u$ über, es ist also $\operatorname{am}(-u) = -\operatorname{am} u$ und folglich

$$\operatorname{sn}(-u) = -\operatorname{sn} u, \quad \operatorname{cn}(-u) = \operatorname{cn} u, \quad \operatorname{dn}(-u) = \operatorname{dn} u,$$

d. h. es ist $\operatorname{sn} u$ eine ungerade, $\operatorname{cn} u$, $\operatorname{dn} u$ sin gerade Funktionen.

Setzt man also

$$\frac{d\varphi_2}{\varDelta\varphi_2} = du, \quad \frac{d\varphi_3}{\varDelta\varphi_3} = dv, \quad \frac{d\varphi_1}{\varDelta\varphi_1} = -d(u+v),$$

so lassen sich die Formeln (17), § 13 anwenden, und man erhält die Additionstheoreme:

$$(6)\qquad \begin{aligned} \operatorname{sn}(u+v) &= \frac{\operatorname{sn} u \operatorname{cn} v \operatorname{dn} v + \operatorname{sn} v \operatorname{cn} u \operatorname{dn} u}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \\ \operatorname{cn}(u+v) &= \frac{\operatorname{cn} u \operatorname{cn} v - \operatorname{sn} u \operatorname{sn} v \operatorname{dn} u \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \\ \operatorname{dn}(u+v) &= \frac{\operatorname{dn} u \operatorname{dn} v - \varkappa^2 \operatorname{sn} u \operatorname{sn} v \operatorname{cn} u \operatorname{cn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}. \end{aligned}$$

Man kann daraus die drei elliptischen Funktionen für beliebige Werte des Arguments eindeutig berechnen, wenn sie für irgend ein noch so kleines Gebiet um den Nullpunkt bestimmt sind. Diesen Satz nimmt Weierstrass zum Ausgangspunkt der Theorie der elliptischen Funktionen.

Setzt man

$$\int_0^{\frac{\pi}{2}} \frac{d\varphi}{\varDelta\varphi} = K,$$

so ist $\operatorname{sn} K = 1$, $\operatorname{cn} K = 0$, $\operatorname{dn} K = \sqrt{1-\varkappa^2} = \varkappa'$, und es ergeben also die Formeln (6), indem man $v = K$ setzt:

$$(7)\qquad \begin{aligned} \operatorname{sn}(u+K) &= \frac{\operatorname{cn} u}{\operatorname{dn} u}, \\ \operatorname{cn}(u+K) &= \frac{-\varkappa' \operatorname{sn} u}{\operatorname{dn} u}, \\ \operatorname{dn}(u+K) &= \frac{\varkappa'}{\operatorname{dn} u}, \end{aligned}$$

und wenn man diese Formel noch einmal anwendet:

$$(8)\qquad \begin{aligned} \operatorname{sn}(u+2K) &= -\operatorname{sn} u, \\ \operatorname{cn}(u+2K) &= -\operatorname{cn} u, \\ \operatorname{dn}(u+2K) &= \operatorname{dn} u, \end{aligned}$$

und abermals angewandt:

$$
(9)\qquad
\begin{aligned}
\operatorname{sn}(u + 4K) &= \operatorname{sn} u,\\
\operatorname{cn}(n + 4K) &= \operatorname{cn} u,\\
\operatorname{dn}(u + 4K) &= \operatorname{dn} u.
\end{aligned}
$$

Es haben also die elliptischen Funktionen die Eigenschaft der Periodizität mit den trigonometrischen Funktionen gemein. Sie haben die Periode $4K$ ($\operatorname{dn} u$ auch die Periode $2K$).

In § 3 haben wir als Beispiel die Transformation, die Formel (1), abgeleitet:

$$
(10)\qquad \frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}} = \frac{dx}{i\sqrt{x(1-x)(1-\varkappa'^2 x)}},
$$

wenn

$$
(11)\qquad z = \frac{-x}{1-x}
$$

war. Setzt man also

$$
\frac{dx}{\sqrt{x(1-x)(1-\varkappa'^2 x)}} = i\,du,
$$

so ist, wenn x und u zugleich verschwinden, $x = \operatorname{sn}^2(iu, \varkappa')$, $1 - x = \operatorname{cn}^2(iu, \varkappa')$, und aus (10) folgt:

$$
\frac{dz}{\sqrt{z(1-z)(1-\varkappa^2 z)}} = du,
$$

also

$$
z = \operatorname{sn}^2(u, \varkappa).
$$

Demnach ergibt (11)

$$
(12)\qquad \operatorname{sn}(u, \varkappa) = \frac{-i\operatorname{sn}(iu, \varkappa')}{\operatorname{cn}(iu, \varkappa')}
$$

(worin das Vorzeichen aus dem speziellen Wert $u = 0$ zu bestimmen ist).

Setzt man nun

$$
\int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{1 - \varkappa'^2 \sin^2\varphi}} = K',
$$

so ergibt sich aus (8)

$$
\begin{aligned}
\operatorname{sn}(iu + 2K', \varkappa') &= -\operatorname{sn}(iu, \varkappa'),\\
\operatorname{cn}(iu + 2K', \varkappa') &= -\operatorname{cn}(iu, \varkappa'),
\end{aligned}
$$

und folglich aus (12)

$$
\operatorname{sn}(u - 2iK', \varkappa) = \operatorname{sn}(u, \varkappa)
$$

oder auch, indem man u in $u + 2iK'$ verwandelt und die Bezeichnung $\varkappa$ wieder wegläßt:

$$\text{(13)} \qquad \operatorname{sn}(u + 2iK') = \operatorname{sn} u.$$

Es hat also die Funktion $\operatorname{sn} u$ eine doppelte Periodizität. Die eine dieser Perioden, $4K$, ist reell die andere, $2iK'$, rein imaginär (wenigstens wenn der Modul $\varkappa$ ein positiver echter Bruch ist). Diese doppelte Periodizität ist eine Eigenschaft, die in dem Gebiete der elementaren Funktionen nirgends vorkommt, und so am deutlichsten zeigte, daß man es hier mit einer neuen Funktionenart zu tun hat. Die aus der doppelten Periodizität abgeleiteten Folgerungen sind es zugleich, die, wie die Erfahrung gezeigt hat, weitaus am schnellsten mit befriedigender Strenge in das Innere der Theorie einführen, so daß hier der zweckmäßigste Ausgangspunkt für eine methodische Entwickelung zu suchen ist. Unsere nächsten Betrachtungen werden daher den doppelt periodischen Funktionen im allgemeinen gewidmet sein

---

Zweiter Abschnitt.

Theta - Funktionen.

§ 15. Voraussetzungen aus der Funktionentheorie.

Der Begriff der doppelt periodischen Funktionen kann nur dann richtig aufgefaßt werden, wenn man sie als Funktionen eines komplexen Arguments $u = v + iw$ betrachtet, worin i wie gewöhnlich die Bedeutung von $\sqrt{-1}$ hat. Die Variable u gilt uns als unabhängige und unbeschränkt veränderliche Größe, die nach dem Vorgange von Gauss durch die Punkte einer Ebene in der Weise geometrisch veranschaulicht wird, daß der Punkt, dessen Koordinaten in einem rechtwinkeligen System v, w sind, als Träger des Wertes $u = v + iw$ angesehen und kurz als der Punkt u bezeichnet wird.

Wir beschränken unsere Betrachtung hier auf eindeutige analytische Funktionen $\varphi(u)$, die im Endlichen keine wesentlich singulären Stellen haben. Was im Unendlichen geschieht, lassen wir dahingestellt. Wir setzen also von den betrachteten Funktionen folgendes voraus:

1. In jedem endlichen Flächenstück liegt eine endliche Anzahl von Punkten, in denen die Funktion $\varphi(u)$ unendlich wird; diese Punkte heißen Unstetigkeitspunkte.

Die Anzahl der Unstetigkeitspunkte überhaupt, d. h. in der ganzen unendlichen Ebene, kann natürlich auch unendlich groß sein.

2. Ist u_0 ein nicht zu den Unstetigkeitspunkten gehöriger Punkt, so ist die Funktion entwickelbar in eine nach ganzen aufsteigenden positiven Potenzen von $u - u_0$ fortschreitende Reihe, die konvergent ist in einem Kreise, der den Punkt u_0 zum Mittelpunkte hat und bis zum nächstgelegenen Unstetigkeitspunkte reicht. Man sagt, die Funktion habe in der Umgebung des Punktes u_0 den Charakter einer ganzen Funktion.

3. Ist u_0 ein Unstetigkeitspunkt, so gibt es eine ganze positive Zahl m von der Art, daß $(u - u_0)^m \varphi(u)$ in dem Punkte u_0 endlich, stetig und von Null verschieden bleibt und daher nach ganzen positiven Potenzen von $u - u_0$ entwickelbar ist. Der Unstetigkeitspunkt wird in diesem Falle von der $m$ten Ordnung genannt. Es ergibt sich daraus eine Entwickelung von $\varphi(u)$ nach steigenden Potenzen von $u - u_0$, die mit $(u - u_0)^{-m}$ anfängt und in einem um u_0 beschriebenen Kreise, der bis zum nächstgelegenen Unstetigkeitspunkte reicht, konvergiert. Der Koeffizient von $(u - u_0)^{-1}$ in dieser Entwickelung heißt das Residuum dieser Funktion für den Punkt u_0.

4. Der Cauchysche Satz. Das Integral

$$\frac{1}{2\pi i}\int \varphi(u)\,du,$$

in positivem Sinne über die Begrenzung eines endlichen Flächenstückes erstreckt, das auf der Randlinie keine Unstetigkeitspunkte enthält, ist gleich der Summe der Residuen für die im Inneren des Flächenstückes liegenden Unstetigkeitspunkte. Als positive Integrationsrichtung ist dabei diejenige anzusehen, die gegen das Innere des Flächenstückes so liegt, wie die v-Achse zur w-Achse, so daß bei der üblichen Bestimmungsweise dieser Achsen beim positiven Durchlaufen des Randes das Innere der Fläche zur Linken bleibt.

5. Die Funktion

$$\psi(u) = \frac{d \log \varphi(u)}{du} = \frac{1}{\varphi(u)}\frac{d\varphi(u)}{du}$$

hat nur Unstetigkeitspunkte erster Ordnung, und wenn in einem Punkte u_0 das Produkt $(u - u_0)^{-m}\varphi(u)$ endlich und von Null verschieden ist, so ist m das Residuum von $\psi(u)$ für diesen Punkt. Ist m positiv, so heißt u_0 ein Nullpunkt $m$ter Ordnung von $\varphi(u)$.

Hiernach ist eine unmittelbare Folgerung des Cauchyschen Theorems:

6. Das Integral

$$\frac{1}{2\pi i}\int d \log \varphi(u),$$

ausgedehnt in positiver Richtung über die Begrenzung eines Flächenstückes, ist gleich der Anzahl der Nullpunkte, vermindert um die Anzahl der Unstetigkeitspunkte, die im Inneren dieses

Flächenstückes liegen, wobei Nullpunkte und Unstetigkeitspunkte $m$ter Ordnung wie m solche Punkte erster Ordnung zu zählen sind. Hieraus folgt, daß im Inneren eines endlichen Flächenstückes auch nur eine endliche Anzahl von Nullpunkten liegt.

In gleichem Sinne ergibt sich

7. Das Integral

$$\frac{1}{2\pi i}\int u\, d\log\varphi(u)$$

ist gleich der Summe der Werte von u, für die $\varphi(u)$ verschwindet, vermindert um die Summe der Werte von u, für die $\varphi(u)$ unendlich wird.

8. Eine Funktion, die im Endlichen gar keine Unstetigkeitspunkte besitzt, heißt eine ganze Funktion. Eine ganze Funktion, die auch im Unendlichen endlich bleibt, ist eine Konstante. Eine ganze Funktion, die auch im Unendlichen keine wesentlich singuläre Stelle hat, für die es also einen Exponenten m derart gibt, daß $u^{-m}\varphi(u)$ für $u = \infty$ nicht unendlich wird, ist eine rationale Funktion.

9. Eine ganze Funktion, deren Reziproke gleichfalls ganz ist, heißt eine Einheitsfunktion. Eine solche Funktion wird im Endlichen weder Unendlich noch Null. Ihr Logarithmus ist daher ebenfalls eine ganze Funktion, und es folgt daraus, daß jede Einheitsfunktion in der Form $e^{g(u)}$ dargestellt werden kann, worin $g(u)$ eine ganze Funktion ist. Umgekehrt ist jeder Ausdruck von dieser Form eine Einheitsfunktion.

10. Nach den grundlegenden Untersuchungen von Weierstrass über die eindeutigen analytischen Funktionen (Abhandlungen der Berliner Akademie von 1876) gibt es immer eine ganze Funktion $G(u)$, die in den Unstetigkeitspunkten einer Funktion $\varphi(u)$ und nur in diesen verschwindet, und diese Funktion $G(u)$ ist durch die Unstetigkeitspunkte von $\varphi(u)$ bis auf eine Einheitsfunktion als Faktor bestimmt. Es ist dann $\varphi(u)\, G(u) = G_1(u)$ gleichfalls eine ganze Funktion, und man kann also jede Funktion $\varphi(u)$ als Quotienten zweier ganzen Funktionen

$$\varphi(u) = \frac{G_1(u)}{G(u)}$$

darstellen, worin $G(u)$ und $G_1(u)$ keine gemeinschaftlichen Nullpunkte haben.

11. Zähler und Nenner dieser Darstellung sind durch $\varphi'(u)$ selbst, abgesehen von Einheitsfaktoren, eindeutig bestimmt.

Die Funktionen $G(u)$, $G_1(u)$ können in Primfaktoren, d. h. in Faktoren zerlegt werden, die nur in einem Punkte Null werden. Verfolgt man diesen Weg bei den doppelt periodischen Funktionen, so gelangt man zu den Weierstrassschen σ-Funktionen. Wir werden aber einen anderen Weg gehen, auf dem wir den σ-Funktionen erst an einer späteren Stelle begegnen.

§ 16. Periodizität.

Eine Funktion $\varphi(u)$ von u, welche die Eigenschaft hat, daß für ein konstantes ω und für jeden Wert von u

$$(1) \qquad \varphi(u+\omega) = \varphi(u)$$

ist, heißt periodisch und ω heißt die Periode.

Der Gegenstand unserer Untersuchung sind Funktionen $\varphi(u)$ mit zwei Perioden ω_1, ω_2, von denen wir ein für allemal voraussetzen wollen, daß ihr Verhältnis $\omega_2:\omega_1$ nicht reell und daß der imaginäre Teil dieses Verhältnisses positiv sei. In der letzteren Annahme liegt nur eine Festsetzung über die Bezeichnung ω_1, ω_2. Denn wenn $\omega_2:\omega_1$ einen negativen imaginären Teil hat, so ist der von $\omega_1:\omega_2$ positiv.

Jede Kombination $m_1\omega_1 + m_2\omega_2$ ist, wenn m_1, m_2 ganze Zahlen sind, gleichfalls eine Periode.

Wir nehmen in der Ebene u einen beliebigen Punkt u_0 an und bezeichnen die vier Punkte

$$u_0, \quad u_0+\omega_1, \quad u_0+\omega_1+\omega_2, \quad u_0+\omega_2;$$

verbinden wir diese vier Punkte der Reihe nach durch gerade Linien, indem wir vom letzten zum ersten zurückkehren, so erhalten wir ein Parallelogramm, welches das Periodenparallelogramm genannt wird. Es können die geradlinigen Seiten des Periodenparallelogramms auch durch krummlinige Züge ersetzt werden, wenn nur die gegenüberliegenden durch Parallelverschiebung zur Deckung gelangen und die einzelnen Züge keine Schleifen bilden.

Ist $\omega_1 = \alpha_1 + \beta_1 i$, $\omega_2 = \alpha_2 + \beta_2 i$ und $\alpha_1, \alpha_2, \beta_1, \beta_2$ reell, so ist nach der Voraussetzung $(\alpha_1\beta_2 - \alpha_2\beta_1)$ positiv, und die geometrische Bedeutung dieser Größe ist (nach bekannten Sätzen

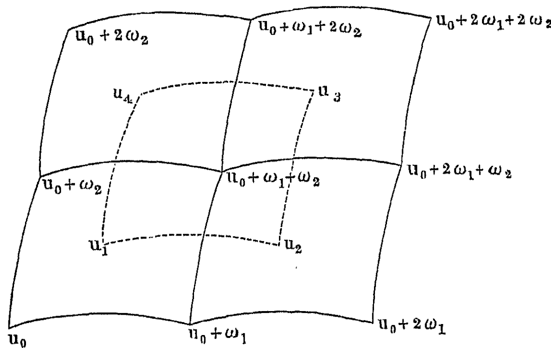
der analytischen Geometrie) der Flächeninhalt des Periodenparallelogramms.

Durch Aneinanderreihen kongruenter Periodenparallelogramme läßt sich die ganze u-Ebene einfach und lückenlos überdecken. Entsprechende Punkte zweier verschiedener dieser Parallelogramme sind die Repräsentanten von u-Werten, die sich um ganzzahlige Vielfache der Perioden unterscheiden, und die nach dem Modul (ω_1, ω_2) kongruent oder, wenn kein Zweifel möglich ist, kurzweg kongruent genannt werden. Das Zeichen der Kongruenz ist

$$u \equiv u' \pmod{\omega_1, \omega_2},$$

und besagt, daß u' die Form $u + m_1 \omega_1 + m_2 \omega_2$ hat, wenn m_1, m_2 ganze Zahlen sind.

Fig. 1.



So stellt die Fig. 1 vier aneinander gelagerte Periodenparallelogramme dar; die Punkte u_1, u_2, u_3, u_4 sind kongruent:

$$u_2 = u_1 + \omega_1, \quad u_3 = u_1 + \omega_1 + \omega_2, \quad u_4 = u_1 + \omega_2,$$

und u_1, u_2, u_3, u_4 bilden ebenfalls die Ecken eines Periodenparallelogramms.

Die doppelt periodische Funktion $\varphi(u)$ hat in allen kongruenten Punkten denselben Wert, und der ganze Wertvorrat dieser Funktion erschöpft sich also in einem Periodenparallelogramm, wenn von zwei gegenüberliegenden Seiten nur die eine mit zum Parallelogramm gerechnet wird.

Wir ziehen aus unseren allgemeinen Voraussetzungen die Folgerung:

1. Es existiert (außer der Konstanten) keine doppelt periodische Funktion, die im Periodenparallelogramm frei von Unstetigkeitspunkten ist; denn eine solche Funk-

tion wäre in der ganzen u-Ebene endlich und müßte also nach § 15, 8 eine Konstante sein.

Ist $\varphi(u)$ eine doppeltperiodische Funktion mit den Perioden ω_1, ω_2, so ist das über die Begrenzung des Periodenparallelogramms genommene Integral [wegen (1)]

$$\int d\log\varphi(u) = \int_{u_0}^{u_0+\omega_1} [d\log\varphi(u) - d\log\varphi(u+\omega_2)]$$
$$-\int_{u_0}^{u_0+\omega_2} [d\log\varphi(u) - d\log\varphi(u+\omega_1)] = 0.$$

Daraus folgt nach § 15, 6. der Satz:

2. Eine doppeltperiodische Funktion wird in einem Periodenparallelogramm in ebenso vielen Punkten Null wie unendlich. Ist m diese Zahl, so heißt m die Ordnung der doppeltperiodischen Funktion. Nach 1. gibt es keine doppeltperiodischen Funktionen von der Ordnung Null.

Ersetzt man in dem Beweise die Funktion $\varphi(u)$ durch $\varphi(u) - c$, so folgt, daß eine doppeltperiodische Funktion $m$ter Ordnung jeden beliebigen Wert c in gleich vielen Punkten annimmt.

Wenn wir das Integral der Formel in 7., § 15 über die Begrenzung des Periodenparallelogramms nehmen, so ergibt sich:

$$\int u\,d\log\varphi(u) = \int_{u_0}^{u_0+\omega_1} [u\,d\log\varphi(u) - (u+\omega_2)\,d\log\varphi(u+\omega_2)]$$
$$-\int_{u_0}^{u_0+\omega_2} [u\,d\log\varphi(u) - (u+\omega_1)\,d\log\varphi(u+\omega_1)]$$
$$= \omega_1 \int_{u_0}^{u_0+\omega_2} d\log\varphi(u) - \omega_2 \int_{u_0}^{u_0+\omega_1} d\log\varphi(u).$$

Nun ist wegen der Mehrdeutigkeit des Logarithmus

$$\int_{u_0}^{u_0+\omega_2} d\log\varphi(u) = \log\varphi(u+\omega_2) - \log\varphi(u) = 2\pi i m_1$$
$$\int_{u_0}^{u_0+\omega_1} d\log\varphi(u) = \log\varphi(u+\omega_1) - \log\varphi(u) = -2\pi i m_2,$$

worin m_1 und m_2 unbestimmte ganze Zahlen sind.

Wenn daher die Funktion $\varphi(u)$ in den Punkten $\alpha_1, \alpha_2, \ldots, \alpha_m$ unendlich, in den Punkten $\beta_1, \beta_2, \ldots, \beta_m$ Null wird, so ist nach § 15, 7.:

$$\Sigma\alpha_i \equiv \Sigma\beta_i \pmod{\omega_1, \omega_2}.$$

Ersetzt man $\varphi(u)$ durch $\varphi(u) - c$, worin c einen beliebigen Wert bedeutet, so folgt der wichtige Satz:

3. Die Summe der Argumentwerte, in denen eine doppeltperiodische Funktion im Inneren eines Periodenparallelogramms einen und denselben Wert c annimmt, ist von c unabhängig oder ändert sich bei stetiger Veränderung von c höchstens sprungweise um eine Periode.

4. Hieraus folgt, daß es auch keine doppeltperiodische Funktion erster Ordnung gibt.

Denn eine solche Funktion müßte jeden Wert c in einem Punkte u annehmen. Ist sie also gleich c' in einem Punkte u' und gleich c'' in einem davon verschiedenen Punkte u'', so würde aus 3. $u' \equiv u''$ folgen, gegen die Voraussetzung.

Unter einer doppeltperiodischen Funktion der zweiten Art versteht man nach Hermite eine Funktion $\psi(u)$, die den Perioden ω_1, ω_2 gegenüber sich den Gleichungen gemäß verhält:

$$\psi(u + \omega_1) = a_1 \psi(u), \qquad \psi(u + \omega_2) = a_2 \psi(u),$$

worin a_1, a_2 Konstanten sind.

5. Auch für eine doppeltperiodische Funktion der zweiten Art gilt der Satz, daß sie in gleich vielen Punkten des Periodenparallelogramms Null und unendlich wird. Ist die Zahl dieser Punkte m, so heißt auch hier die Funktion von der $m$ten Ordnung.

Der Beweis ist derselbe wie der des Satzes 2. Es gilt aber hier nicht mehr die Erweiterung, daß die Funktion $\psi(u)$ jeden Wert gleich oft annimmt, weil $\psi(u) - c$ jetzt nicht mehr periodisch ist.

6. Eine doppeltperiodische Funktion $\psi(u)$ von der zweiten Art und der Ordnung Null ist notwendig eine Konstante oder eine Exponentialfunktion. Denn wenn $\psi(u)$ nicht Null wird, so ist

$$\varphi(u) = \frac{\psi'(u)}{\psi(u)}$$

eine doppeltperiodische Funktion von der ersten Art, die nicht unendlich wird, also nach 1. eine Konstante a. Daraus folgt:

$$\psi(u) = A e^{au},$$

worin A eine neue Konstante ist.

§ 17. Die Funktionen T.

Wenn doppeltperiodische Funktionen $\varphi(u)$ von der $m$ten Ordnung existieren, so müssen es gebrochene Funktionen sein. Setzen wir sie also nach § 15, 10. in der Form

$$\varphi(u) = \frac{G_1(u)}{G(u)}, \tag{1}$$

wenn $G_1(u)$ und $G(u)$ ganze Funktionen ohne gemeinsamen Nullpunkt sind, so ist

$$\frac{G_1(u+\omega_1)}{G(u+\omega_1)} = \frac{G_1(u+\omega_2)}{G(u+\omega_2)} = \frac{G_1(u)}{G(u)},$$

und darin haben die drei Funktionen $G(u)$, $G(u+\omega_1)$, $G(u+\omega_2)$ dieselben m Nullpunkte, nämlich die Unstetigkeitspunkte von $\varphi(u)$. Ihre Quotienten sind also Einheitsfunktionen, und nach § 15, 9. ist also, wenn $g_1(u)$, $g_2(u)$ ganze Funktionen sind:

$$\begin{aligned} G(u+\omega_1) &= e^{g_1(u)}\, G(u), \\ G(u+\omega_2) &= e^{g_2(u)}\, G(u), \end{aligned} \tag{2}$$

und die Funktion $G_1(u)$ genügt den nämlichen Gleichungen.

Ist

$$\varphi(u) = \frac{T_1(u)}{T(u)} \tag{3}$$

eine zweite Darstellung von $\varphi(u)$ von der Form (1), so ist

$$T(u) = e^{g(u)}\, G(u), \tag{4}$$

worin $g(u)$ wieder eine ganze Funktion ist, und wenn also nach (2)

$$\begin{aligned} T(u+\omega_1) &= e^{l_1(u)}\, T(u), \\ T(u+\omega_2) &= e^{l_2(u)}\, T(u) \end{aligned} \tag{5}$$

ist, so ist

$$\begin{aligned} g_1(u) &= l_1(u) + g(u) - g(u+\omega_1), \\ g_2(u) &= l_2(u) + g(u) - g(u+\omega_2). \end{aligned}$$

Es kommt also alles darauf an, daß wir unter irgend einer passenden Annahme über die ganzen Funktionen $l_1(u)$, $l_2(u)$ ganze Funktionen $T(u)$ bilden können, die den Bedingungen (5) genügen und in m beliebig gegebenen Punkten des Periodenparallelogramms verschwinden. Durch die Quotienten zweier solcher Funktionen mit denselben $l_1(u)$, $l_2(u)$ können wir dann alle doppeltperiodischen Funktionen $\varphi(u)$ darstellen, und die allgemeineren Funktionen $G(u)$, die dasselbe leisten, erhält man nach (4) durch Hinzufügung eines willkürlichen Einheitsfaktors.

Wollten wir $l_1(u)$, $l_2(u)$ als Konstanten annehmen, so wäre $T(u)$ eine ganze doppeltperiodische Funktion der zweiten Art und folglich nach § 16, 6. eine Exponentialfunktion, aus der sich keine doppeltperiodischen Funktionen bilden lassen. Die einfachste Annahme, die uns hiernach bleibt, ist die, daß $l_1(u)$, $l_2(u)$ lineare Funktionen von u sind, worunter als Spezialfall auch der enthalten ist, daß eine der beiden Funktionen l_1, l_2 konstant ist.

Wir stellen also die folgende Definition auf:

1. Eine T-Funktion, $T(u)$, ist eine ganze Funktion von u, die den folgenden beiden Gleichungen genügt:

$$(6) \qquad \begin{aligned} T(u + \omega_1) &= e^{-\pi i[a_1(2u+\omega_1)+b_1]}\, T(u), \\ T(u + \omega_2) &= e^{-\pi i[a_2(2u+\omega_2)+b_2]}\, T(u). \end{aligned}$$

Hierin sind a_1, b_1, a_2, b_2 Konstanten, d. h. von u unabhängige Größen. Die Perioden ω_1, ω_2 gelten hier durchweg als ein für allemal gegebene Konstanten, deren Verhältnis $\omega_2 : \omega_1$ einen positiven imaginären Teil hat.

Die Faktoren

$$\begin{aligned} e_1 &= e_1(u) = e^{-\pi i[a_1(2u+\omega_1)+b_1]}, \\ e_2 &= e_2(u) = e^{-\pi i[a_2(2u+\omega_2)+b_2]} \end{aligned}$$

heißen die beiden Periodizitätsfaktoren der Funktion T.

Die Periodizitätsfaktoren ändern sich nicht, wenn b_1, b_2 um gerade ganze Zahlen verändert werden. Daß es Funktionen dieser Art wirklich gibt, wird sich erst im weiteren Verlaufe der Untersuchung ergeben.

2. Wenn die Funktion $T(u)$ in irgend einem Punkte verschwindet, so verschwindet sie auch in allen kongruenten Punkten. Verschwindet sie in m Punkten des Periodenparallelogramms, so heißt sie von der $m$ten Ordnung.

Aus dieser Definition ergibt sich sofort:

3. Durch Multiplikation zweier T-Funktionen T, T' der Ordnung m, m' erhält man eine T-Funktion der Ordnung $m + m'$. Die Periodizitätsfaktoren des Produktes T, T' sind die Produkte der Periodizitätsfaktoren von T und T'.

Wir fragen zunächst nach der Möglichkeit von T-Funktionen nullter Ordnung: Ist $L(u)$ eine solche und $L'(u)$ ihre Ableitung, so folgt durch zweimalige Differentiation von (6)

$$\frac{d}{du}\frac{L'(u+\omega_1)}{L(u+\omega_1)} = \frac{d}{du}\frac{L'(u)}{L(u)},$$

und entsprechend aus der zweiten Gleichung (6). Danach ist $d^2 \log L(u)/du^2$ als ganze doppeltperiodische Funktion eine Konstante, und folglich $\log L(u)$ eine ganze Funktion zweiten Grades von u. Wir erhalten also:

4. Eine T-Funktion nullter Ordnung ist von der Form

$$(7) \qquad L(u) = Ce^{-\pi i(\lambda u^2 + \mu u)},$$

worin λ, μ, C Konstanten sind.

Daß jede Funktion dieser Form eine T-Funktion nullter Ordnung ist, ersieht man ohne weiteres.

Das Produkt

$$(8) \qquad T'(u) = L(u)\,T(u)$$

ist ebenso wie $T(u)$ eine T-Funktion $m$ter Ordnung und verschwindet in denselben Punkten.

Die Periodizitätsfaktoren von T' erhält man aus denen von T, wenn man die Exponenten a_1, a_2, b_1, b_2 durch

$$(9) \qquad \begin{aligned} a_1' &= a_1 + \lambda\omega_1, & b_1' &= b_1 + \mu\omega_1 \\ a_2' &= a_2 + \lambda\omega_2, & b_2' &= b_2 + \mu\omega_2 \end{aligned}$$

ersetzt, worin die b, b' jedoch nur bis auf additive gerade ganze Zahlen bestimmt sind.

5. Nach (9) kann man μ immer und nur auf eine Weise so bestimmen, daß b_1', b_2' reell werden.

Denn setzt man die imaginären Teile von b_1', b_2' gleich Null, so erhält man für den imaginären und reellen Teil von μ zwei lineare Gleichungen, deren Determinante nach § 16 der Flächeninhalt des Periodenparallelogramms, also von Null verschieden ist.

Die Periodizitätsfaktoren und die Nullpunkte einer T-Funktion $m$ter Ordnung stehen in einer gewissen Abhängigkeit voneinander, die wir leicht aus den Sätzen des § 15 erhalten. Zunächst ergibt sich die Ordnung m, wenn man das Integral

$$\frac{1}{2\pi i}\int d\log T(u) = m$$

über die Begrenzung des Periodenparallelogramms ausdehnt. Legt man der Einfachheit halber die Ecke u_0 (Fig. 1) in den Koordinatenanfangspunkt, so kann man dieses Integral so zerlegen:

$$2\pi i m = \int_0^{\omega_1} d[\log T(u) - \log T(u+\omega_2)]$$
$$- \int_0^{\omega_2} d[\log T(u) - \log T(u+\omega_1)]$$

und nach (6) ist

$$d[\log T(u) - \log T(u+\omega_2)] = 2\pi i a_2,$$
$$d[\log T(u) - \log T(u+\omega_1)] = 2\pi i a_1.$$

Daraus ergibt sich

(10) $$a_2\omega_1 - a_1\omega_2 = m.$$

Bezeichnen wir weiter mit $\alpha_1, \alpha_2, \ldots, \alpha_m$ die Nullpunkte einer T-Funktion im Innern eines Periodenparallelogramms, so erhalten wir aus § 15, 7.

$$2\pi i \Sigma\alpha = \int u\, d\log Tu,$$

wenn das Integral wieder über die Begrenzung des Parallelogramms erstreckt wird. Es ist aber

$$\int u\, d\log Tu = \int_0^{\omega_1} [u\, d\log Tu - (u+\omega_2)\, d\log T(u+\omega_2)]$$
$$- \int_0^{\omega_2} [u\, d\log Tu - (u+\omega_1)\, d\log T(u+\omega_1)],$$

und das erste dieser beiden Integrale ist nach (6)

$$-\omega_2 \int_0^{\omega_1} d\log T(u) + 2\pi i a_2 \int_0^{\omega_1} (u+\omega_2)\, du$$
$$= -\omega_2[\log T(\omega_1) - \log T(0)] + \pi i a_2\omega_1(\omega_1 + 2\omega_2)$$
$$= \pi i \omega_2(a_1\omega_1 + b_1) + \pi i a_2(\omega_1^2 + 2\omega_1\omega_2) + 2\pi i N_2\omega_2,$$

worin N_2 (wegen der Vieldeutigkeit des Logarithmus) eine nicht näher bestimmte ganze Zahl ist. Ebenso ergibt sich für das zweite der Integrale:

$$-\pi i \omega_1(a_2\omega_2 + b_2) - \pi i a_1(\omega_2^2 + 2\omega_1\omega_2) + 2\pi i N_1\omega_1,$$

und folglich (als Kongruenz geschrieben)

(11) $$\Sigma\alpha \equiv \frac{1}{2}(b_1\omega_2 - b_2\omega_1) + \frac{m}{2}(\omega_1 + \omega_2).$$

Diese Summe oder vielmehr die Gesamtheit der damit nach dem Modul (ω_1, ω_2) kongruenten Zahlen heißt der Charakter der T-Funktion.

Der Charakter der Funktion T ändert sich nicht, wenn man T durch eine der Funktionen LT ersetzt (nach 8.). Man kann also nach 5. den Charakter auch in der Form darstellen:

$$(12) \qquad \Sigma a \equiv \frac{1}{2}(g_1 \omega_2 - g_2 \omega_1) + \frac{m}{2}(\omega_1 + \omega_2),$$

worin g_1, g_2 reell sind. Diese reellen Zahlen sind durch den Charakter bis auf Vielfache von 2 bestimmt und können jeden Wert zwischen 0 und 2 haben. Das Symbol (g_1, g_2) heißt die Charakteristik der T-Funktion. Aus der Charakteristik wird der Charakter der T-Funktion nach (12) bestimmt.

Ist γ der Charakter einer Funktion $T(u)$ von der Ordnung m und v eine beliebige Konstante, so hat $T(u + v)$ den Charakter

$$\gamma' \equiv \gamma - vm.$$

Hiernach lassen sich, wenn $m > 0$ ist, die verschiedenen Charaktere aufeinander zurückführen.

Mit Hilfe der Gleichung (10) kann man die beiden Gleichungen (6) in eine allgemeine zusammenfassen:

Wenn man in der ersten Gleichung (6) wiederholt u in $u + \omega_1$ verwandelt, so erhält man das System:

$$\begin{aligned} T(u + \omega_1) &= e^{-\pi i [a_1(2u + \omega_1) + b_1]}\, T(u), \\ T(u + 2\omega_1) &= e^{-\pi i [a_1(2u + 3\omega_1) + b_1]}\, T(u + \omega_1), \\ &\dots\dots\dots\dots\dots \\ T(u + n_1\omega_1) &= e^{-\pi i [a_1(2u + (2n_1 - 1)\omega_1) + b_1]}\, T[u + (n_1 - 1)\omega_1], \end{aligned}$$

und durch Multiplikation aller dieser Formeln:

$$(13) \qquad T(u + n_1\omega_1) = e^{-\pi i [a_1(2n_1 u + n_1^2 \omega_1) + n_1 b_1]}\, T(u).$$

Diese Formel ist zunächst für ein positives ganzzahliges n_1 abgeleitet. Ersetzt man aber darin u durch $u - n_1\omega_1$, so ergibt sich ihre Richtigkeit auch für negative n_1.

Ebenso ergibt sich:

$$(14) \qquad T(u + n_2\omega_2) = e^{-\pi i [a_2(2n_2 u + n_2^2 \omega_2) + n_2 b_2]}\, T(u),$$

und wenn man in dieser Formel u in $u + n_1\omega_1$ verwandelt und wieder (13) anwendet:

$$(15) \qquad \begin{aligned} &T(u + n_1\omega_1 + n_2\omega_2) \\ &= e^{-\pi i [2(a_1 n_1 + a_2 n_2) u + 2 a_2 n_1 n_2 \omega_1 + a_1 n_1^2 \omega_1 + a_2 n_2^2 \omega_2 + n_1 b_1 + n_2 b_2]}\, T(u). \end{aligned}$$

Es ist aber nach (10)

$$2 a_2 n_1 n_2 \omega_1 = a_1 n_1 n_2 \omega_1 + a_2 n_1 n_2 \omega_2 + m n_1 n_2,$$

und demnach wird diese letzte Formel:

$$(16) \quad \begin{aligned} &T(u + n_1 \omega_1 + n_2 \omega_2) \\ &= e^{-\pi i [(n_1 a_1 + n_2 a_2)(2u + n_1 \omega_1 + n_2 \omega_2) + \pi i (b_1 n_1 + b_2 n_2 + m n_1 n_2)]} T(u). \end{aligned}$$

Und hierin sind n_1 und n_2 beliebige ganze positive oder negative Zahlen.

Wenn man zwei T-Funktionen der Ordnung m und m' von den Charakteren γ, γ' miteinander multipliziert, so entsteht eine neue T-Funktion, deren Ordnung $m + m'$ und deren Charakter $\gamma + \gamma'$ ist. Sind (g_1, g_2) und (g'_1, g'_2) die Charakteristiken der beiden Faktoren, so ist $(g_1 + g'_1, g_2 + g'_2)$ die Charakteristik des Produktes.

§ 18. Relationen zwischen verwandten T-Funktionen.

Zwei T-Funktionen von den gleichen Perioden, derselben Ordnung und demselben Charakter wollen wir verwandt nennen. Ist $T'(u)$ eine mit $T(u)$ verwandte T-Funktion und haben a'_1, a'_2, b'_1, b'_2 dieselbe Bedeutung für T', wie a_1, a_2, b_1, b_2 für T, so ist infolge der vorausgesetzten Verwandtschaft [§ 17, (10), (11)]:

$$(1) \quad a'_1 \omega_2 - a'_2 \omega_1 = a_1 \omega_2 - a_2 \omega_1,$$

$$(2) \quad b'_1 \omega_2 - b'_2 \omega_1 = b_1 \omega_2 - b_2 \omega_1 + 2 n_1 \omega_2 - 2 n_2 \omega_1,$$

worin n_1, n_2 ganze Zahlen sind.

Daher lassen sich λ und μ nach § 17, (9) so bestimmen, daß die Periodizitätsfaktoren der Funktion

$$e^{-\pi i (\lambda u^2 + \mu u)} T(u)$$

dieselben werden wie die der Funktion $T'(u)$, und daher haben wir den Satz:

1. Verwandten T-Funktionen können durch Hinzufügung einer T-Funktion nullter Ordnung:

$$L = C e^{-\pi i (\lambda u^2 + \mu u)}$$

als Faktor dieselben Periodizitätsfaktoren gegeben werden.

Ferner folgt unmittelbar aus der Gleichheit der Charaktere:

2. Wenn verwandte T-Funktionen $m$ter Ordnung $m - 1$ gemeinsame Nullpunkte im Periodenparallelogramm haben, so haben sie auch den $m$ten gemeinsam; und hieraus:

3. Zwischen höchstens $m+1$ verwandten T-Funktionen $m$ter Ordnung $T, T_1, \ldots, T_m$ besteht eine identische Gleichung von der Form

$$LT + L_1 T_1 + \cdots + L_m T_m = 0.$$

Denn besteht diese Relation nicht bereits für $L = 0$, so kann man von den in $L_1, L_2, \ldots, L_m$ verfügbaren Konstanten zunächst $\lambda_1, \lambda_2 \ldots, \lambda_m, \mu_1, \mu_2 \ldots, \mu_m$ so bestimmen, daß die sämtlichen Produkte $L_1 T_1, L_2 T_2, \ldots, L_m T_m$ dieselben Periodizitätsfaktoren erhalten, und dann die $C_1, C_2, \ldots, C_m$ so, daß $m-1$ und folglich alle Nullpunkte der Funktion $L_1 T_1 + L_2 T_2 + \cdots + L_m T_m$ mit den Nullpunkten der Funktion T zusammenfallen. Daraus aber folgt, daß das Verhältnis von $L_1 T_1 + L_2 T_2 + \cdots + L_m T_m$ zu T gleich einer T^0-Funktion $-L$ ist, was zu beweisen ist.

4. Die Quotienten verwandter T-Funktionen können durch Hinzufügung eines Faktors L in doppeltperiodische Funktionen verwandelt werden.

5. Setzen wir die Existenz einer T-Funktion erster Ordnung $t(u)$ voraus, so läßt sich daraus jede T-Funktion $m$ter Ordnung ableiten.

Es sei nämlich γ der Charakter von $t(u)$ und $\alpha_1, \alpha_2, \ldots, \alpha_m$ beliebig gegebene Werte. Es verschwindet dann die Funktion

$$t(u - \alpha_i + \gamma) = t_i(u), \qquad i = 1, 2, \ldots m$$

in dem Punkte α_i und allen mit α_i kongruenten Punkten, aber in keinem anderen.

Das Produkt

$$T(u) = t_1(u) t_2(u) \ldots t_m(u)$$

ist also eine T-Funktion $m$ter Ordnung mit den beliebig gegebenen Nullpunkten $\alpha_1, \alpha_2, \ldots, \alpha_m$.

6. Hieraus läßt sich leicht beweisen, daß jede doppeltperiodische Funktion, die in einem Periodenparallelogramm nur eine endliche Anzahl von Unstetigkeitspunkten hat, als Quotient zweier T-Funktionen darstellbar ist.

Es sei nämlich $\varphi(u)$ eine doppeltperiodische Funktion mit den Perioden ω_1, ω_2 und den Unstetigkeitspunkten $\alpha_1, \alpha_2, \ldots, \alpha_m$, die auch teilweise in Unstetigkeitspunkte höherer Ordnung zusammenfallen können.

Bestimmt man nach 5. eine Funktion $T(u)$ mit den Nullpunkten $\alpha_1, \alpha_2, \ldots, \alpha_m$, so ist:

$$T(u)\varphi(u) = T_1(u)$$

eine T-Funktion $m$ter Ordnung, und

$$\varphi(u) = \frac{T_1(u)}{T(u)} \qquad w. z. b. w.$$

Die Funktionen $T(u)$, $T_1(u)$ sind verwandt, da sie dieselben Periodizitätsfaktoren und also auch dieselbe Charakteristik haben.

Die Nullpunkte von $T_1(u)$ sind zugleich die Nullpunkte von $\varphi(u)$, und die Summe dieser Nullwerte ist also kongruent mit der Summe der Unstetigkeitswerte.

§ 19. T-Funktionen erster Ordnung.

Wir gehen nun dazu über, die T-Funktionen erster Ordnung, die wir mit $t(u)$ bezeichnen, aus denen sich die übrigen T-Funktionen, wie wir gesehen haben, ableiten lassen, näher zu bestimmen.

Aus 3. des vorigen Paragraphen folgt, daß zwei t-Funktionen derselben Charakteristik sich nur durch einen Faktor von der Form

$$C e^{-\pi i(\lambda u^2 + \mu u)}$$

voneinander unterscheiden, und wir wollen nun durch eine Erweiterung der Definition diesen Faktor noch näher bestimmen.

Dies soll, was nach § 17, (9) ohne Beschränkung der Allgemeinheit möglich ist, so geschehen, daß in den Periodizitätsfaktoren

$$a_1 = 0, \quad b_1 = g_1, \quad b_2 = g_2$$

wird, wenn (g_1, g_2) die Charakteristik ist; wegen der Relation

$$a_2\omega_1 - a_1\omega_2 = 1$$

ist dann

$$a_2 = \frac{1}{\omega_1},$$

und die Bedingungen für diese t-Funktion lauten alsdann (§ 17, 1.):

$$(1) \qquad \begin{aligned} t(u + \omega_1) &= e^{-\pi i g_1} t(u), \\ t(u + \omega_2) &= e^{-\pi i \frac{2u + \omega_2}{\omega_1}} e^{-\pi i g_2} t(u), \end{aligned}$$

und hierdurch ist die Funktion $t(u)$ bis auf einen von u unabhängigen Faktor bestimmt. Um diesen Faktor noch näher zu

bestimmen, fassen wir die Abhängigkeit der Funktion t auch von ω_1, ω_2 ins Auge und bezeichnen sie, indem wir g_1, g_2 als gegebene von ω_1, ω_2 unabhängige Zahlen betrachten, mit $t(u, \omega_1, \omega_2)$. Es zeigt sich dann, daß, wenn h ein willkürlicher Faktor ist,

$$t(hu, h\omega_1, h\omega_2)$$

gleichfalls den Bedingungen (1) genügt, und daß demnach

$$\frac{t(hu, h\omega_1, h\omega_2)}{t(u, \omega_1, \omega_2)} = f(\omega_1, \omega_2) \tag{2}$$

von u unabhängig ist.

Die Funktion $f(\omega_1, \omega_2)$ kann aber immer in die Form gesetzt werden:

$$f(\omega_1, \omega_2) = \frac{\varphi(h\omega_1, h\omega_2)}{\varphi(\omega_1, \omega_2)};$$

man hat nur, wenn $t(u)$ für $u = 0$ nicht verschwindet:

$$\varphi(\omega_1, \omega_2) = t(0, \omega_1, \omega_2),$$

und wenn $t(0) = 0$ ist, etwa

$$\varphi(\omega_1, \omega_2) = \omega_1 t'(0, \omega_1, \omega_2)$$

zu setzen, wenn t' die Derivierte von t nach u bezeichnet. Indem man also jetzt

$$\frac{t(u, \omega_1, \omega_2)}{\varphi(\omega_1, \omega_2)} \tag{3}$$

wieder mit $t(u, \omega_1, \omega_2)$ bezeichnet, kann man den Bedingungen (1) noch die hinzufügen, daß für ein beliebiges h

$$t(u, \omega_1, \omega_2) = t(hu, h\omega_1\, h\omega_2). \tag{4}$$

Die Funktion t hängt also jetzt nur noch von zwei Veränderlichen, nämlich den Verhältnissen $u : \omega_1 : \omega_2$, ab. Wir setzen in (4)

$$h = \frac{1}{\omega_1}, \quad \frac{u}{\omega_1} = v, \quad \frac{\omega_2}{\omega_1} = \omega,$$

und erhalten

$$t(u, \omega_1, \omega_2) = t\left(\frac{u}{\omega_1}, 1, \frac{\omega_2}{\omega_1}\right) = \vartheta(v, \omega), \tag{5}$$

worin ϑ ein neues Funktionszeichen ist.

Hierdurch ist also eine neue Funktion $\vartheta(v)$ definiert von nur zwei Variablen v, ω, deren erste unbeschränkt veränderlich ist, während ω nach der im § 16 gemachten Voraussetzung einen positiven imaginären Bestandteil hat; v heißt das Argument, ω der Modul der ϑ-Funktion.

§ 20. Die ϑ-Funktion.

Die Funktion $\vartheta(v)$ ist eine ganze Funktion von v, die den Bedingungen genügt:

$$(1)\qquad \begin{aligned}\vartheta(v+1) &= e^{-\pi i g_1}\vartheta(v),\\ \vartheta(v+\omega) &= e^{-\pi i(2v+\omega)}e^{-\pi i g_2}\vartheta(v),\end{aligned}$$

und ist dadurch bis auf einen von v unabhängigen Faktor bestimmt. Sie ist also unter den t-Funktionen als Spezialfall enthalten, während andererseits die allgemeine t-Funktion durch die ϑ-Funktion ausgedrückt werden kann in der Weise:

$$t(u) = Ce^{-\pi i(\lambda u^2+\mu u)}\vartheta\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right),$$

worin C, λ, μ beliebige konstante oder von ω_1, ω_2 abhängige Größen sind.

Die Funktion ϑ ist noch von den in der Charakteristik vorkommenden Zahlen g_1, g_2 abhängig, und wenn eine Bezeichnung dieser Abhängigkeit erforderlich ist, so soll für $\vartheta(v, \omega)$:

$$\vartheta_{g_1, g_2}(v, \omega)$$

gesetzt werden, es können dabei g_1, g_2 beliebige Zahlen sein. Nach dem früheren genügt es, wenn wir sie reell und zwischen 0 und 2 annehmen.

Entsprechend den T-Funktionen höherer Ordnung werden wir auch Θ-Funktionen $m$ter Ordnung einführen und verstehen darunter eine ganze Funktion von v, die den Bedingungen genügt:

$$(2)\qquad \begin{aligned}\Theta(v+1) &= e^{-\pi i g_1}\Theta(v)\\ \Theta(v+\omega) &= e^{-m\pi i(2v+\omega)}e^{-\pi i g_2}\Theta(v).\end{aligned}$$

Auch hierbei kann die Charakteristik g_1, g_2 in die Bezeichnung mit aufgenommen werden:

$$\Theta_{g_1, g_2}(v, \omega).$$

Diese Funktionen sind als spezielle Fälle unter den T-Funktionen enthalten, und man kann allgemeine T-Funktionen in der Weise bilden:

$$(3)\qquad Ce^{-\pi i(\lambda u^2+\mu u)}\Theta\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right).$$

Es ergibt sich also aus § 18, 3. der Fundamentalsatz für die Θ-Funktionen, den wir folgendermaßen aussprechen:

Nennen wir Θ-Funktionen mit denselben Perioden gleicher Ordnung und gleicher Charakteristik verwandt, und bezeichnen wir ferner ein System von Funktionen als linear abhängig oder unabhängig, je nachdem eine homogene lineare Relation mit konstanten (nicht sämtlich verschwindenden) Koeffizienten zwischen diesen Funktionen besteht oder nicht besteht, so gilt der Satz:

> $m + 1$ verwandte Θ-Funktionen $m$ter Ordnung sind immer linear abhängig;

oder:

> Aus m linear unabhängigen verwandten Θ-Funktionen $m$ter Ordnung läßt sich jede andere verwandte Θ-Funktion linear (mit konstanten Koeffizienten) zusammensetzen.

Dieser Satz ist für unsere folgenden Betrachtungen von der fundamentalsten Bedeutung; es ergibt sich daraus nach § 18, 3., daß jede T-Funktion $m$ter Ordnung mit Anwendung der Formel (3) aus m linear unabhängigen Θ-Funktionen zusammengesetzt werden kann.

Nach § 17, (11) ist die Summe der m Argumentwerte, für welche die Funktion $\Theta_{g_1, g_2}(v)$ im Periodenparallelogramm verschwindet, nach dem Modul $(1, \omega)$ kongruent mit

$$m \frac{1 + \omega}{2} + \frac{g_1 \omega - g_2}{2}.$$

Die bis jetzt gegebene Definition der Funktion ϑ läßt einen Faktor, der eine Funktion von ω sein kann, unbestimmt. Wir können aber durch einen Zusatz zur Definition diesen Faktor noch näher bestimmen.

Wenn man die Definitionsgleichungen (1) zweimal nach v und einmal nach ω differentiiert, indem man g_1, g_2 als konstant ansieht, so ergibt sich nach einfacher Rechnung, daß die Funktion

$$\frac{\partial^2 \vartheta(v, \omega)}{\partial v^2} - 4 \pi i \frac{\partial \vartheta(v, \omega)}{\partial \omega}$$

selbst den Bedingungen (1) genügt und also die Form

$$\varphi(\omega) \vartheta(v, \omega)$$

hat, worin $\varphi(\omega)$ in bezug auf v konstant, also eine Funktion von ω allein ist. Wenn man jetzt

$$e^{-\frac{1}{4\pi i}\int \varphi(\omega)\, d\omega} \vartheta(v, \omega)$$

gleich einem neuen ϑ setzt, so ergibt sich für dieses die partielle Differentialgleichung

$$(4) \qquad \frac{\partial^2 \vartheta(v, \omega)}{\partial v^2} - 4\pi i \frac{\partial \vartheta(v, \omega)}{\partial \omega} = 0,$$

und durch (1) und (4) ist jetzt die Funktion ϑ bis auf einen von v und ω unabhängigen, also nur noch von g_1, g_2 abhängigen Faktor definiert.

§ 21. Die Theta-Funktionen verschiedener Charakteristiken. Hauptcharakteristiken.

Wir wollen jetzt, ehe wir an die Bestimmung des noch übrigen von v und ω unabhängigen Faktors in den ϑ-Funktionen gehen, die verschiedenen Charakteristiken aufeinander zurückführen, was nach § 17 immer möglich ist. Bezeichnet man mit $\vartheta(v)$ die zur Charakteristik (0, 0) gehörige ϑ-Funktion, so ist

$$\Phi(v, \omega) = e^{-\pi i g_1 v}\, \vartheta\left(v - \frac{g_1 \omega - g_2}{2}\right)$$

eine den Bedingungen (1) § 20 genügende Funktion. Es ist aber nun mit Rücksicht auf die Differentialgleichung (4):

$$\frac{\partial^2 \Phi}{\partial v^2} - 4\pi i \frac{\partial \Phi}{\partial \omega} = -\pi^2 g_1^2 \Phi,$$

und wenn wir also

$$(1) \qquad \vartheta_{g_1, g_2}(v) = e^{\frac{\pi i \omega g_1^2}{4} - \pi i g_1 v + \frac{g_1 g_2 \pi i}{2}}\, \vartheta\left(v - \frac{g_1 \omega - g_2}{2}\right)$$

setzen, so ist die Differentialgleichung (4) § 20 durch alle diese Funktionen befriedigt. Hierdurch also sind die Funktionen ϑ_{g_1, g_2} bis auf einen allen gemeinschaftlichen numerischen Faktor bestimmt.

Aus der Formel (1) läßt sich eine allgemeinere ableiten, indem man v durch $v - \frac{g_1' \omega - g_2'}{2}$ ersetzt. Man erhält so

$$(2) \qquad \vartheta_{g_1, g_2}\left(v - \frac{g_1' \omega - g_2'}{2}\right) = e^{-\frac{\pi i \omega}{4} g_1'^2 + \pi i g_1' v - \pi i g_1 g_2' - \frac{\pi i}{2} g_1' (g_2 + g_2')}\, \vartheta_{g_1 + g_1', g_2 + g_2'}(v).$$

Aus (2) ergibt sich noch, mit Benutzung von (1) § 20, wenn man $g_1' = 2$, $g_2' = 0$, oder $g_1' = 0$, $g_2' = 2$ setzt:

$$(3) \qquad \begin{aligned} \vartheta_{g_1+2, g_2}(v) &= e^{2\pi i g_2} \vartheta_{g_1, g_2}(v), \\ \vartheta_{g_1, g_2+2}(v) &= e^{\pi i g_1} \vartheta_{g_1, g_2}(v), \end{aligned}$$

und durch (2) ist also zugleich die Periodizität der Funktionen $\vartheta_{g_1, g_2}(v)$ vollständig ausgedrückt. Beispielsweise ergibt sich, wenn μ und ν ganze Zahlen sind:

$$(4) \qquad \begin{aligned} &\vartheta_{00}\left(v - \frac{(2\nu - 1)\omega + 2\mu - 1}{2}\right) \\ &= (-1)^{\nu+1} i \, e^{\frac{-\pi i \omega}{4}(2\nu-1)^2} e^{\pi i (2\nu-1) v} \vartheta_{11}(v). \end{aligned}$$

$$(5) \qquad \vartheta_{11}(v - \nu\omega - \mu) = (-1)^{\mu+\nu} e^{-\pi i \omega \nu^2} e^{2\pi i \nu v} \vartheta_{11}(v).$$

Die Formel (2) ist gültig für ganz beliebige, selbst komplexe Werte von g_1, g_2.

Wenn man in den Definitionsformeln der ϑ-Funktionen [§ 20, (1)] v durch $-v-1$, und durch $-v-\omega$, ferner g_1, g_2 durch $-g_1$, $-g_2$ ersetzt, so zeigt sich, daß $\vartheta_{-g_1,-g_2}(-v)$ denselben Bedingungen genügt, wie $\vartheta_{g_1,g_2}(v)$, und daß sonach

$$\vartheta_{g_1,g_2}(v), \quad \vartheta_{-g_1,-g_2}(-v)$$

bis auf einen konstanten Faktor identisch sind; es ist also insbesondere, wie aus $v = 0$ hervorgeht:

$$\vartheta_{0,0}(v) = \vartheta_{0,0}(-v),$$

und danach ergibt die Formel (1), wenn man v, g_1, g_2 durch $-v$, $-g_1$, $-g_2$ ersetzt:

$$(6) \qquad \vartheta_{g_1,g_2}(v) = \vartheta_{-g_1,-g_2}(-v).$$

Sind die Elemente g_1, g_2 ganze Zahlen, so heißt (g_1, g_2) eine Hauptcharakteristik. Es gibt deren vier wesentlich verschiedene, nämlich:

$$(0,0), \quad (0,1), \quad (1,0), \quad (1,1),$$

und demnach auch vier wesentlich verschiedene Haupt-ϑ-Funktionen:

$$(7) \qquad \vartheta_{00}(v), \quad \vartheta_{01}(v), \quad \vartheta_{10}(v), \quad \vartheta_{11}(v),$$

von denen die erste auch mit $\vartheta(v)$ bezeichnet wird.

In der Folge werden unter Charakteristiken und ϑ-Funktionen nur noch Hauptcharakteristiken und Hauptfunktionen verstanden.

Die Formel (2), auf dies Funktionensystem angewandt, ergibt die folgende, häufig benutzte Tabelle:

$$
(8)\quad
\begin{aligned}
\vartheta_{00}(v) &= \vartheta_{01}(v+\tfrac{1}{2}) = \varepsilon\vartheta_{10}\left(v+\frac{\omega}{2}\right) = \varepsilon\vartheta_{11}\left(v+\frac{1+\omega}{2}\right),\\
\vartheta_{01}(v) &= \vartheta_{00}(v+\tfrac{1}{2}) = -i\varepsilon\vartheta_{11}\left(v+\frac{\omega}{2}\right) = i\varepsilon\vartheta_{10}\left(v+\frac{1+\omega}{2}\right),\\
\vartheta_{10}(v) &= \vartheta_{11}(v+\tfrac{1}{2}) = \varepsilon\vartheta_{00}\left(v+\frac{\omega}{2}\right) = \varepsilon\vartheta_{01}\left(v+\frac{1+\omega}{2}\right),\\
\vartheta_{11}(v) &= -\vartheta_{10}(v+\tfrac{1}{2}) = -i\varepsilon\vartheta_{01}\left(v+\frac{\omega}{2}\right) = -i\varepsilon\vartheta_{11}\left(v+\frac{1+\omega}{2}\right),
\end{aligned}
$$

worin zur Abkürzung

$$
\varepsilon = e^{\frac{\pi i\omega}{4} + \pi i v}
$$

gesetzt ist.

Nach (3), (4) ist

$$
(9)\quad
\begin{aligned}
\vartheta_{00}(-v) &= \vartheta_{00}(v), & \vartheta_{01}(-v) &= \vartheta_{01}(v),\\
\vartheta_{10}(-v) &= \vartheta_{10}(v), & \vartheta_{11}(-v) &= -\vartheta_{11}(v),
\end{aligned}
$$

d. h. es sind $\vartheta_{00}(v)$, $\vartheta_{01}(v)$, $\vartheta_{10}(v)$ gerade Funktionen, $\vartheta_{11}(v)$ ist eine ungerade Funktion.

Nach § 17 (12) verschwinden die vier Funktionen (7), bzw. für die folgenden Werte des Arguments

$$
\frac{1+\omega}{2},\ \frac{\omega}{2},\ \frac{1}{2},\ 0,
$$

also für gewisse halbe Perioden. Von Wichtigkeit sind die Werte, welche die sämtlichen Funktionen (7) für diese Argumentwerte annehmen, und diese lassen sich mittels der Tabelle (8) auf die drei

$$
\vartheta_{00}(0) = \vartheta_{00},\quad \vartheta_{01}(0) = \vartheta_{01},\quad \vartheta_{10}(0) = \vartheta_{10}
$$

zurückführen. Man erhält so aus (8) das folgende System von Formeln:

$$
(10)\quad
\begin{aligned}
\vartheta_{00} &= \vartheta_{01}\left(\frac{1}{2}\right) = \varepsilon_0\vartheta_{10}\left(\frac{\omega}{2}\right) = \varepsilon_0\vartheta_{11}\left(\frac{1+\omega}{2}\right),\\
\vartheta_{01} &= \vartheta_{00}\left(\frac{1}{2}\right) = -i\varepsilon_0\vartheta_{11}\left(\frac{\omega}{2}\right) = i\varepsilon_0\vartheta_{10}\left(\frac{1+\omega}{2}\right),\\
\vartheta_{10} &= \vartheta_{11}\left(\frac{1}{2}\right) = \varepsilon_0\vartheta_{00}\left(\frac{\omega}{2}\right) = \varepsilon_0\vartheta_{01}\left(\frac{1+\omega}{2}\right),
\end{aligned}
$$

worin

$$\varepsilon_0 = e^{\frac{\pi i \omega}{4}}$$

und

(11) $\vartheta_{11}(0) = 0,\ \vartheta_{10}\left(\frac{1}{2}\right) = 0,\ \vartheta_{01}\left(\frac{\omega}{2}\right) = 0,\ \vartheta_{00}\left(\frac{1+\omega}{2}\right) = 0.$

Die Quadrate der Funktionen (7):

(12) $$\vartheta_{00}^2(v),\ \vartheta_{01}^2(v),\ \vartheta_{10}^2(v),\ \vartheta_{11}^2(v)$$

sind Θ_{00}-Funktionen zweiter Ordnung, und folglich bestehen zwischen ihnen zwei lineare Relationen. Nehmen wir diese Relationen in der Form an:

$$\vartheta_{10}^2(v) = A\,\vartheta_{01}^2(v) + B\,\vartheta_{11}^2(v),$$
$$\vartheta_{00}^2(v) = A'\vartheta_{01}^2(v) + B'\vartheta_{11}^2(v),$$

so kann man die Koeffizienten auf Grund der Formeln (10), (11) leicht bestimmen, wenn man $v = 0$ und $v = \frac{\omega}{2}$ setzt. Man erhält so

(13) $$\begin{aligned}\vartheta_{01}^2\,\vartheta_{10}^2(v) &= \vartheta_{10}^2\,\vartheta_{01}^2(v) - \vartheta_{00}^2\,\vartheta_{11}^2(v),\\ \vartheta_{01}^2\,\vartheta_{00}^2(v) &= \vartheta_{00}^2\,\vartheta_{01}^2(v) - \vartheta_{10}^2\,\vartheta_{11}^2(v),\end{aligned}$$

und daraus noch, indem man $v = \frac{1}{2}$ setzt:

(14) $$\vartheta_{00}^4 = \vartheta_{01}^4 + \vartheta_{10}^4.$$

Durch zwei beliebige von den Quadraten (12) können alle Funktionen Θ_{00} der zweiten Ordnung linear dargestellt werden; aber auch die übrigen Θ-Funktionen zweiter Ordnung lassen sich aus den Funktionen ϑ_{g_1,g_2} zusammensetzen, denn man erhält für jede Charakteristik zwei linear unabhängige Produkte, von denen das eine eine gerade, das andere eine ungerade Funktion ist, nämlich:

(15)

$\vartheta_{00}(v)\,\vartheta_{01}(v),\quad \vartheta_{10}(v)\,\vartheta_{11}(v)$	Charakteristik	(0,1)
$\vartheta_{00}(v)\,\vartheta_{10}(v),\quad \vartheta_{01}(v)\,\vartheta_{11}(v)$	„	(1,0)
$\vartheta_{10}(v)\,\vartheta_{01}(v),\quad \vartheta_{00}(v)\,\vartheta_{11}(v)$	„	(1,1)

Nach demselben Prinzip lassen sich nun alle Θ-Funktionen beliebiger Ordnung und beliebiger Hauptcharakteristik aus den Funktionen ϑ bilden. Um dies nachzuweisen, bezeichnen wir mit Θ_0, Θ_1 irgend zwei der ϑ-Quadrate (12) und mit $F^{(n)}(\Theta_0, \Theta_1)$ eine ganze rationale und homogene Funktion $n$ter Ordnung der beiden Argumente Θ_0, Θ_1. Man erhält hiernach für die Θ-Funktionen $m$ter Ordnung $\Theta^{(m)}(v)$ folgende Ausdrücke:

m gerade gerade Funktionen

$$\Theta^{(m)}_{00}(v) = F^{\left(\frac{m}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{01}(v) = \vartheta_{00}(v)\,\vartheta_{01}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{10}(v) = \vartheta_{00}(v)\,\vartheta_{10}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{11}(v) = \vartheta_{10}(v)\,\vartheta_{01}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$

(16) ungerade Funktionen

$$\Theta^{(m)}_{00}(v) = \vartheta_{00}(v)\,\vartheta_{10}(v)\,\vartheta_{01}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-4}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{01}(v) = \vartheta_{10}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{10}(v) = \vartheta_{01}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{11}(v) = \vartheta_{00}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m}{2}-1\right)}(\Theta_0, \Theta_1)$$

m ungerade gerade Funktionen

$$\Theta^{(m)}_{00}(v) = \vartheta_{00}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{01}(v) = \vartheta_{01}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{10}(v) = \vartheta_{10}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{11}(v) = \vartheta_{00}(v)\,\vartheta_{01}(v)\,\vartheta_{10}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$

(17) ungerade Funktionen

$$\Theta^{(m)}_{00}(v) = \vartheta_{01}(v)\,\vartheta_{10}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{01}(v) = \vartheta_{00}(v)\,\vartheta_{10}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{10}(v) = \vartheta_{00}(v)\,\vartheta_{01}(v)\,\vartheta_{11}(v)\,F^{\left(\frac{m-3}{2}\right)}(\Theta_0, \Theta_1)$$
$$\Theta^{(m)}_{11}(v) = \vartheta_{11}(v)\,F^{\left(\frac{m-1}{2}\right)}(\Theta_0, \Theta_1).$$

Daß in dieser Form alle Θ-Funktionen darstellbar sind, ergibt sich auf Grund von § 20 aus folgenden drei Erwägungen.

1. Zwischen geraden und ungeraden Funktionen kann keine lineare Abhängigkeit bestehen, wenn nicht schon zwischen den geraden Funktionen für sich oder den ungeraden für sich eine lineare Abhängigkeit besteht.

2. Da zwei der ϑ-Quadrate (12) nicht in konstantem Verhältnis stehen, so besteht auch keine Gleichung von der Form $F^{(n)}(\Theta_0, \Theta_1) = 0$.

3. Die Gesamtzahl der Konstanten, die nach (16), (17) in den zu einer und derselben Charakteristik gehörenden geraden und ungeraden Funktionen auftreten, ist genau gleich der Ordnung m.

§ 22. Das Additionstheorem.

Sind u, v zwei Veränderliche, so gehören die Produkte

$$\vartheta_{g_1, g_2}(u + v)\,\vartheta_{g'_1, g'_2}(u - v)$$

zu den Θ-Funktionen zweiter Ordnung, mit der Charakteristik

$$(g_1 + g'_1,\ g_2 + g'_2),$$

und zwar für jede der beiden Variablen u, v; sie sind also als Funktionen von v linear darstellbar durch die Funktionen (12) und (15) in § 21, so daß die Variable u in den Koeffizienten vorkommt. Diese Darstellung ist, wenn die Charakteristik (0, 0) ist, auf mehrfache Art möglich, da man zwei beliebige der Funktionen (12) wählen kann, in den anderen Fällen nur auf eine Art. Man erhält so 16 Formeln, von denen aber 6 durch bloße Vertauschung von v mit $-v$ aus den anderen herzuleiten sind, so daß nur 10 wesentlich verschiedene bleiben. Man leitet diese Formeln sehr leicht ab, indem man sie zunächst mit unbestimmten Koeffizienten ansetzt und diese dann dadurch bestimmt, daß man für v solche spezielle Werte setzt, für die je eine der Funktionen $\vartheta(v)$ verschwindet. So ist z. B.:

$$\vartheta_{00}(u + v)\,\vartheta_{00}(u - v) = A\,\vartheta_{00}^2(v) + B\,\vartheta_{11}^2(v),$$

und wenn man $v = 0$ und $v = \frac{1 + \omega}{2}$ setzt, so erhält man mit Benutzung der Formeln des § 21:

$$A\,\vartheta_{00}^2 = \vartheta_{00}^2(u), \quad B\,\vartheta_{00}^2 = \vartheta_{11}^2(u),$$

also

$$(1)\quad \vartheta_{00}^2\,\vartheta_{00}(u + v)\,\vartheta_{00}(u - v) = \vartheta_{00}^2(u)\,\vartheta_{00}^2(v) + \vartheta_{11}^2(u)\,\vartheta_{11}^2(v),$$

und wenn man hierin u durch

$$u + \frac{1}{2}, \quad u + \frac{\omega}{2}, \quad u + \frac{1 + \omega}{2}$$

ersetzt, so bildet man drei weitere Relationen, die man auf demselben Wege wie (1) auch direkt hätte ableiten können:

(2) $\vartheta_{01}^2\, \vartheta_{01}(u+v)\,\vartheta_{01}(u-v) = \vartheta_{01}^2(u)\,\vartheta_{01}^2(v) - \vartheta_{11}^2(u)\,\vartheta_{11}^2(v)$.

(3) $\vartheta_{10}^2\, \vartheta_{10}(u+v)\,\vartheta_{10}(u-v) = \vartheta_{10}^2(u)\,\vartheta_{10}^2(v) - \vartheta_{11}^2(u)\,\vartheta_{11}^2(v)$.

(4) $\vartheta_{01}^2\, \vartheta_{11}(u+v)\,\vartheta_{11}(u-v) = \vartheta_{11}^2(u)\,\vartheta_{01}^2(v) - \vartheta_{01}^2(u)\,\vartheta_{11}^2(v)$.

Diese vier Gleichungen können, wie schon erwähnt, durch Anwendung der Formeln (13) des vorigen Paragraphen in mannigfacher Weise umgeformt werden. Die folgenden sechs Formeln haben nur eine Form. Es ist, um wieder mit einem beliebigen Beispiel zu beginnen:

$$\vartheta_{00}(u+v)\,\vartheta_{11}(u-v) = A\,\vartheta_{01}(v)\,\vartheta_{10}(v) + B\,\vartheta_{00}(v)\,\vartheta_{11}(v),$$

und wenn man $v = 0$ setzt:

$$A\,\vartheta_{01}\,\vartheta_{10} = \vartheta_{00}(u)\,\vartheta_{11}(u),$$

daraus erhält man B durch Vertauschung von u mit v. So sind die drei folgenden Formeln abgeleitet:

(5) $$\vartheta_{01}\vartheta_{10}\vartheta_{00}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{10}(v) - \vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{11}(v),$$

(6) $$\vartheta_{00}\vartheta_{01}\vartheta_{10}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{10}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{01}(v) - \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{10}(v)\vartheta_{11}(v),$$

(7) $$\vartheta_{00}\vartheta_{10}\vartheta_{01}(u+v)\vartheta_{11}(u-v)$$
$$= \vartheta_{01}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{10}(v) - \vartheta_{00}(u)\vartheta_{10}(u)\vartheta_{01}(v)\vartheta_{11}(v),$$

die sich unmittelbar verifizieren lassen, indem man erst u, dann $v = 0$ setzt. Hieraus folgen die drei anderen durch Vermehrung von u um

$$\frac{1}{2},\quad \frac{\omega}{2},\quad \frac{1}{2}:$$

(8) $$\vartheta_{01}\vartheta_{10}\vartheta_{01}(u+v)\vartheta_{10}(u-v)$$
$$= \vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{01}(v)\vartheta_{10}(v) + \vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{00}(v)\vartheta_{11}(v),$$

(9) $$\vartheta_{00}\vartheta_{01}\vartheta_{00}(u+v)\vartheta_{01}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{01}(u)\vartheta_{00}(v)\vartheta_{01}(v) - \vartheta_{10}(u)\vartheta_{11}(u)\vartheta_{10}(v)\vartheta_{11}(v),$$

(10) $$\vartheta_{00}\vartheta_{10}\vartheta_{00}(u+v)\vartheta_{10}(u-v)$$
$$= \vartheta_{00}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{10}(v) + \vartheta_{01}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{11}(v).$$

Es lassen sich diese Formeln, deren Gesamtheit mit dem Namen des Additionstheorems bezeichnet wird, in mannigfacher Weise verallgemeinern, wovon das folgende als Beispiel dienen möge.

Sind u, v zwei Variable, so sind die vier Produkte

$$\vartheta_{00}(u)\vartheta_{00}(u+v), \qquad \vartheta_{01}(u)\vartheta_{01}(u+v),$$
$$\vartheta_{10}(u)\vartheta_{10}(u+v), \qquad \vartheta_{11}(u)\vartheta_{11}(u+v),$$

als Funktionen von u betrachtet, verwandte T-Funktionen zweiter Ordnung mit den gleichen Periodizitätsfaktoren, und daher sind je drei von ihnen linear abhängig. Es ist also

$$A\vartheta_{00}(u)\vartheta_{00}(u+v) + B\vartheta_{10}(u)\vartheta_{10}(u+v) + C\vartheta_{11}(u)\vartheta_{11}(u+v) = 0,$$

woraus für $u = 0$, $u = \frac{1}{2}$:

$$A\vartheta_{00}\vartheta_{00}(v) + B\vartheta_{10}\vartheta_{10}(v) = 0$$
$$A\vartheta_{01}\vartheta_{01}(v) + C\vartheta_{10}\vartheta_{10}(v) = 0$$

und daraus:

$$(11)\quad \vartheta_{10}\vartheta_{10}(v)\vartheta_{00}(u)\vartheta_{00}(u+v) - \vartheta_{00}\vartheta_{00}(v)\vartheta_{10}(u)\vartheta_{10}(u+v) - \vartheta_{01}\vartheta_{01}(v)\vartheta_{11}(u)\vartheta_{11}(u+v) = 0.$$

Ebenso sind nun auch, wenn w eine dritte Variable ist, die in der Form

$$\vartheta_{g_1,g_2}(u+v)\vartheta_{g_1,g_2}(u+w), \quad \vartheta_{g_1,g_2}(u)\vartheta_{g_1,g_2}(u+v+w)$$

enthaltenen Produkte, als Funktionen von u betrachtet, verwandte T-Funktionen zweiter Ordnung mit den gleichen Periodizitätsfaktoren, so daß zwischen je dreien unter ihnen eine lineare Abhängigkeit besteht. Die Koeffizienten bestimmt man wie oben durch spezielle Werte von u. So folgt das Formelsystem:

$$(12)\quad \begin{aligned} &\vartheta_{00}\vartheta_{00}(v+w)\vartheta_{00}(u+v)\vartheta_{00}(u+w) \\ &= \vartheta_{00}(u)\vartheta_{00}(v)\vartheta_{00}(w)\vartheta_{00}(u+v+w) \\ &- \vartheta_{11}(u)\vartheta_{11}(v)\vartheta_{11}(w)\vartheta_{11}(u+v+w). \end{aligned}$$

$$(13)\quad \begin{aligned} &\vartheta_{01}\vartheta_{01}(v+w)\vartheta_{01}(u+v)\vartheta_{01}(u+w) \\ &= \vartheta_{01}(u)\vartheta_{01}(v)\vartheta_{01}(w)\vartheta_{01}(u+v+w) \\ &+ \vartheta_{11}(u)\vartheta_{11}(v)\vartheta_{11}(w)\vartheta_{11}(u+v+w). \end{aligned}$$

$$(14)\quad \begin{aligned} &\vartheta_{10}\vartheta_{10}(v+w)\vartheta_{10}(u+v)\vartheta_{10}(u+w) \\ &= \vartheta_{10}(u)\vartheta_{10}(v)\vartheta_{10}(w)\vartheta_{10}(u+v+w) \\ &+ \vartheta_{11}(u)\vartheta_{11}(v)\vartheta_{11}(w)\vartheta_{11}(u+v+w). \end{aligned}$$

Alle diese Formeln können als spezielle Fälle einer allgemeinen Formel aufgefaßt werden, die Jacobi aus den Reihenentwickelungen abgeleitet und zur Begründung der Theorie der elliptischen Funktionen verwandt hat[1]). Diese Formel läßt sich auch folgendermaßen aus dem Begriffe der Thetafunktionen gewinnen.

[1]) Theorie der elliptischen Funktionen, aus den Eigenschaften der Thetareihen abgeleitet. Jacobis gesammelte Werke, Bd. I, S. 497.

Die vier Funktionen

(15) $$\vartheta_{00}(2v),\quad \vartheta_{01}(2v),\quad \vartheta_{10}(2v),\quad \vartheta_{11}(2v),$$

sind Θ_{00}-Funktionen vierter Ordnung von v, und da sie linear unabhängig sind, so lassen sich alle Θ_{00}-Funktionen vierter Ordnung linear durch sie ausdrücken. Eine solche Funktion ist aber auch das Produkt

(16) $$\vartheta(v+a_1)\,\vartheta(v+a_2)\,\vartheta(v+a_3)\,\vartheta(v+a_4),$$

vorausgesetzt, daß die Größen a der Bedingung

(17) $$a_1+a_2+a_3+a_4=0$$

genügen. Wir erhalten also, wenn wir mit A_1, A_2, A_3, A_4 Konstanten (in bezug auf v) bezeichnen:

$$\vartheta(v+a_1)\,\vartheta(v+a_2)\,\vartheta(v+a_3)\,\vartheta(v+a_4)$$
$$=A_1\vartheta_{00}(2v)+A_2\vartheta_{01}(2v)+A_3\vartheta_{10}(2v)+A_4\vartheta_{11}(2v),$$

und daraus erhält man durch Vermehrung von v um $\frac{1}{2}(g_1\omega+g_2)$ vier Formeln:

$$\vartheta_{g_1,g_2}(v+a_1)\,\vartheta_{g_1,g_2}(v+a_2)\,\vartheta_{g_1,g_2}(v+a_3)\,\vartheta_{g_1,g_2}(v+a_4)$$
$$=A_1\vartheta_{00}(2v)+(-1)^{g_2}A_2\vartheta_{01}(2v)+(-1)^{g_1}A_3\vartheta_{10}(2v)$$
$$+(-1)^{g_1+g_2}A_4\vartheta_{11}(2v).$$

Wenn man diese vier Formeln addiert, so folgt:

(18) $$4A_1\vartheta_{00}(2v)=\sum^{g_1,g_2}\vartheta_{g_1,g_2}(v+a_1)\,\vartheta_{g_1,g_2}(v+a_2)\,\vartheta_{g_1,g_2}(v+a_3)\,\vartheta_{g_1,g_2}(v+a_4),$$

wo in der Summe für g_1 und g_2 alle Kombinationen von 0 und 1 zu setzen sind.

Wir führen jetzt eine etwas andere Bezeichnung ein, indem wir setzen:

$$v+a_1=v_1',\quad v+a_2=v_2',\quad v+a_3=v_3',\quad v+a_4=v_4',$$

also wegen (17)

$$4v=v_1'+v_2'+v_3'+v_4',$$

und definieren jetzt die vier Größen v_1, v_2, v_3, v_4 durch die Gleichungen

(19) $$\begin{aligned} v_1&=\tfrac{1}{2}(v_1'+v_2'+v_3'+v_4'),\\ v_2&=\tfrac{1}{2}(v_1'+v_2'-v_3'-v_4'),\\ v_3&=\tfrac{1}{2}(v_1'-v_2'+v_3'-v_4'),\\ v_4&=\tfrac{1}{2}(v_1'-v_2'-v_3'+v_4'). \end{aligned}$$

Hieraus erhält man aber:

$$
(20)\quad \begin{aligned}
v_1' &= \tfrac{1}{2}(v_1 + v_2 + v_3 + v_4), & a_1 &= \tfrac{1}{2}(\ \ v_2 + v_3 + v_4),\\
v_2' &= \tfrac{1}{2}(v_1 + v_2 - v_3 - v_4), & a_2 &= \tfrac{1}{2}(\ \ v_2 - v_3 - v_4),\\
v_3' &= \tfrac{1}{2}(v_1 - v_2 + v_3 - v_4), & a_3 &= \tfrac{1}{2}(-v_2 + v_3 - v_4),\\
v_4' &= \tfrac{1}{2}(v_1 - v_2 - v_3 + v_4), & a_4 &= \tfrac{1}{2}(-v_2 - v_3 + v_4),
\end{aligned}
$$

und danach ergibt die Formel (18):

$$4 A_1 \vartheta_{00}(v_1) = \sum \vartheta_{g_1, g_2}(v_1') \vartheta_{g_1, g_2}(v_2') \vartheta_{g_1, g_2}(v_3') \vartheta_{g_1, g_2}(v_4'),$$

worin nun entweder die v_i oder die v_i' als unabhängige Variable angesehen werden können.

Betrachtet man die v_i als unabhängige Variable, so ist in dieser Formel A_1 von v_1 unabhängig, wohl aber noch von v_2, v_3, v_4 abhängig. Setzen wir daher $4 A_1 = c \vartheta_{00}(v_2) \vartheta_{00}(v_3) \vartheta_{00}(v_4)$, so ergibt sich

$$
\begin{aligned}
&c \vartheta_{00}(v_1) \vartheta_{00}(v_2) \vartheta_{00}(v_3) \vartheta_{00}(v_4)\\
&= \sum \vartheta_{g_1, g_2}(v_1') \vartheta_{g_1, g_2}(v_2') \vartheta_{g_1, g_2}(v_3') \vartheta_{g_1, g_2}(v_4'),
\end{aligned}
$$

und darin ist c jedenfalls von v_1 unabhängig. Da nun aber die rechte Seite dieser Formel bei beliebigen Vertauschungen von v_1, v_2, v_3, v_4 ungeändert bleibt, so ist c von allen v_i unabhängig, und man erhält seinen Wert, wenn man alle $v_i = 0$ setzt:

$$c \vartheta_{00}^4 = \vartheta_{00}^4 + \vartheta_{01}^4 + \vartheta_{10}^4,$$

woraus nach § 21, (14) $c = 2$ folgt.

Wir haben also die Formel:

$$
\begin{aligned}
&2 \vartheta_{00}(v_1) \vartheta_{00}(v_2) \vartheta_{00}(v_3) \vartheta_{00}(v_4)\\
&= \sum_{g_1, g_2} \vartheta_{g_1, g_2}(v_1') \vartheta_{g_1, g_2}(v_2') \vartheta_{g_1, g_2}(v_3') \vartheta_{g_1, g_2}(v_4').
\end{aligned}
$$

Wenn man darin jede der Variablen v_1, v_2, v_3, v_4 um eine halbe Periode $-\frac{1}{2}(g_1' \omega_1 - g_2')$ vermehrt, so wird v_1' um eine ganze Periode $-(g_1' \omega_1 - g_2')$ vermehrt, während v_2', v_3', v_4' ungeändert bleiben, und demnach erhält man mit Hilfe von § 21, (2) und (3) ein System von vier Formeln:

$$
(21)\quad
\begin{aligned}
&2 \vartheta_{g'_1, g'_2}(v_1) \vartheta_{g'_1, g'_2}(v_2) \vartheta_{g'_1, g'_2}(v_3) \vartheta_{g'_1, g'_2}(v_4)\\
&= \sum_{g_1, g_2} (-1)^{g_1 g'_2 + g_2 g'_1 + g'_1 g'_2} \vartheta_{g_1, g_2}(v_1') \vartheta_{g_1, g_2}(v_2') \vartheta_{g_1, g_2}(v_3') \vartheta_{g_1, g_2}(v_4').
\end{aligned}
$$

Dies sind die Jacobischen Formeln.

Setzt man z. B.

$$
\begin{aligned}
v_1 &= 0, & v_2 &= v + w, & v_3 &= u + v, & v_4 &= u + w,\\
v_1' &= u + v + w, & v_2' &= -u, & v_3' &= -w, & v_4' &= -v,
\end{aligned}
$$

so ergibt sich aus (21) für $g'_1, g'_2 = 1,1$:

$$0 = \sum^{g_1, g_2} (-1)^{g_1 + g_2} \vartheta_{g_1, g_2}(u) \vartheta_{g_1, g_2}(v) \vartheta_{g_1, g_2}(w) \vartheta_{g_1, g_2}(u + v + w),$$

und hieraus erhält man dann, wenn man in (21) für g'_1, g'_2 die drei anderen Charakteristiken setzt, die Formeln (12), (13), (14).

§ 23. Die Derivierten der ϑ-Funktionen.

Wir bezeichnen im folgenden durch $\vartheta'_{g_1, g_2}(v)$, $\vartheta''_{g_1, g_1}(v)$ die nach v genommenen Derivierten der Funktion $\vartheta_{g_1, g_2}(v)$, und mit ϑ'_{g_1, g_2}, ϑ''_{g_1, g_2} die Werte dieser Funktion für $v = 0$. Es verschwinden dann ϑ'_{01}, ϑ'_{10}, ϑ'_{00}, weil $\vartheta_{01}(v)$, $\vartheta_{10}(v)$, $\vartheta_{00}(v)$ gerade Funktionen von v sind, und ebenso verschwindet ϑ''_{11}.

Die sechs Funktionen

$$\vartheta_{g_1, g_2}(v) \vartheta'_{g'_1, g'_2}(v) - \vartheta_{g'_1, g'_2}(v) \vartheta'_{g_1, g_2}(v)$$

sind, wie aus den Fundamentalgleichungen § 20, (1) hervorgeht, ϑ-Funktionen zweiter Ordnung mit der Charakteristik

$$(g_1 + g'_1,\ g_2 + g'_2),$$

und zugleich entweder gerade oder ungerade Funktionen, wonach sie sich nach § 21 durch ϑ-Funktionen darstellen lassen. Ein konstanter Faktor wird durch einen speziellen Wert von $v\ (v = 0)$ bestimmt. So ist

$$(1) \qquad \vartheta'_{11}(v) \vartheta_{01}(v) - \vartheta'_{01}(v) \vartheta_{11}(v) = A \vartheta_{10}(v) \vartheta_{00}(v).$$

$$(2) \qquad A = \frac{\vartheta'_{11} \vartheta_{01}}{\vartheta_{10} \vartheta_{00}}.$$

Dieser Ausdruck für A läßt sich aber noch vereinfachen.

Differentiieren wir (1) zweimal nach v und setzen dann $v = 0$, so folgt

$$\vartheta'''_{11} \vartheta_{01} - \vartheta''_{01} \vartheta'_{11} = A(\vartheta''_{10} \vartheta_{00} + \vartheta_{10} \vartheta''_{00}),$$

und wenn man für A den Wert (2) einführt:

$$(3) \qquad \frac{\vartheta'''_{11}}{\vartheta'_{11}} = \frac{\vartheta''_{01}}{\vartheta_{01}} + \frac{\vartheta''_{10}}{\vartheta_{10}} + \frac{\vartheta''_{00}}{\vartheta_{00}}.$$

Nun genügen aber [nach § 20, (4)] die vier Funktionen ϑ'_{11}, ϑ_{01}, ϑ_{10}, ϑ_{00} der Differentialgleichung

$$(4) \qquad \vartheta'' = 4 \pi i \frac{\partial \vartheta}{\partial \omega},$$

und danach läßt sich (3) so schreiben:

$$\frac{d \log \vartheta'_{11}}{d \omega} = \frac{d \log \vartheta_{00} \vartheta_{10} \vartheta_{01}}{d \omega},$$

oder durch Integration:

$$\vartheta'_{11} = c\,\vartheta_{00}\vartheta_{10}\vartheta_{01},$$

worin c von ω unabhängig ist. Durch § 20, 21 waren die ϑ-Funktionen bestimmt bis auf einen von v, ω unabhängigen, allen gemeinschaftlichen Faktor. Über diesen Faktor soll nun so verfügt werden, daß die Konstante c den Wert π erhält, also die Formel besteht:

$$(5) \qquad \vartheta'_{11} = \pi\,\vartheta_{00}\vartheta_{10}\vartheta_{01},$$

und dadurch sind jetzt die ϑ-Funktionen bis auf das gemeinschaftliche Vorzeichen $\pm$ vollständig definiert. Durch Anwendung von (5) läßt sich der Formel (1) die Gestalt geben:

$$(6) \qquad \vartheta'_{11}(v)\vartheta_{01}(v) - \vartheta'_{01}(v)\vartheta_{11}(v) = \pi\vartheta^2_{01}\vartheta_{10}(v)\vartheta_{00}(v),$$

und ebenso erhält man mit Benutzung von § 21, (8):

$$(7) \qquad \vartheta'_{11}(v)\vartheta_{00}(v) - \vartheta'_{00}(v)\vartheta_{11}(v) = \pi\vartheta^2_{00}\vartheta_{10}(v)\vartheta_{01}(v),$$

$$(8) \qquad \vartheta'_{11}(v)\vartheta_{10}(v) - \vartheta'_{10}(v)\vartheta_{11}(v) = \pi\vartheta^2_{10}\vartheta_{01}(v)\vartheta_{00}(v),$$

$$(9) \qquad \vartheta'_{10}(v)\vartheta_{01}(v) - \vartheta'_{01}(v)\vartheta_{10}(v) = -\pi\vartheta^2_{00}\vartheta_{00}(v)\vartheta_{11}(v),$$

$$(10) \qquad \vartheta'_{00}(v)\vartheta_{01}(v) - \vartheta'_{01}(v)\vartheta_{00}(v) = -\pi\vartheta^2_{10}\vartheta_{10}(v)\vartheta_{11}(v),$$

$$(11) \qquad \vartheta'_{00}(v)\vartheta_{10}(v) - \vartheta'_{10}(v)\vartheta_{00}(v) = \pi\vartheta^2_{01}\vartheta_{01}(v)\vartheta_{11}(v).$$

Differentiieren wir die Gleichungen (9), (10), (11) nach v und setzen $v = 0$, so erhalten wir mittels (4) und (5) die Relationen

$$(12) \qquad 4\frac{d}{d\omega}\log\frac{\vartheta_{10}}{\vartheta_{01}} = i\pi\vartheta^4_{00},$$

$$(13) \qquad 4\frac{d}{d\omega}\log\frac{\vartheta_{00}}{\vartheta_{01}} = i\pi\vartheta^4_{10},$$

$$(14) \qquad 4\frac{d}{d\omega}\log\frac{\vartheta_{10}}{\vartheta_{00}} = i\pi\vartheta^4_{01}.$$

Wenn man die Fundamentformeln für die ϑ-Funktionen zweimal logarithmisch differentiiert, so erkennt man, daß die Funktionen

$$\vartheta^2(v)\frac{d^2\log\vartheta(v)}{dv^2} = \vartheta''(v)\vartheta(v) - \vartheta'(v)\vartheta'(v)$$

Θ-Funktionen zweiter Ordnung mit der Charakteristik (0, 0) sind, und man kann sie daher durch die Funktionen $\vartheta^2(v)$ linear ausdrücken. Auf diese Weise ergibt sich

$$(15)\qquad \vartheta_{00}^2\vartheta_{00}^2(v)\frac{d^2\log\vartheta_{00}(v)}{dv^2} = \vartheta_{00}\vartheta_{00}''\vartheta_{00}^2(v) + \vartheta_{11}'^2\vartheta_{11}^2(v),$$

$$(16)\qquad \vartheta_{01}^2\vartheta_{01}^2(v)\frac{d^2\log\vartheta_{01}(v)}{dv^2} = \vartheta_{01}\vartheta_{01}''\vartheta_{01}^2(v) - \vartheta_{11}'^2\vartheta_{11}^2(v),$$

$$(17)\qquad \vartheta_{10}^2\vartheta_{10}^2(v)\frac{d^2\log\vartheta_{10}(v)}{dv^2} = \vartheta_{10}\vartheta_{10}''\vartheta_{10}^2(v) - \vartheta_{11}'^2\vartheta_{11}^2(v),$$

$$(18)\qquad \vartheta_{00}^2\vartheta_{11}^2(v)\frac{d^2\log\vartheta_{11}(v)}{dv^2} = \vartheta_{00}\vartheta_{00}''\vartheta_{11}^2(v) - \vartheta_{11}'^2\vartheta_{00}^2(v).$$

Hieraus lassen sich noch weitere Relationen herleiten durch fortgesetzte Differentiation. Wir führen noch eine dieser Formeln an, die sich ergibt, wenn man (15) noch zweimal nach v differentiiert und dann $v = 0$ setzt. Drückt man die Differentiationen nach v durch solche nach ω aus mittels der partiellen Differentialgleichung (4), so folgt:

$$\frac{d^2\log\vartheta_{00}}{d\omega^2} - 2\left(\frac{d\log\vartheta_{00}}{d\omega}\right)^2 = -\frac{\pi^2}{8}\vartheta_{10}^4\vartheta_{01}^4,$$

oder

$$(19)\qquad \frac{d}{d\omega}\left(\frac{1}{\vartheta_{00}^4}\frac{d\vartheta_{00}^2}{d\omega}\right) = -\frac{\pi^2}{4}\frac{\vartheta_{10}^4\vartheta_{01}^4}{\vartheta_{00}^2}.$$

§ 24. Darstellung der ϑ-Funktionen durch unendliche Produkte.

Die Theorie der ϑ-Funktionen ist nun so weit gefördert, daß sich ihre Darstellung sehr leicht ergibt. Damit wird dann die Existenz dieser Funktionen nachgewiesen und die bisherigen Betrachtungen erhalten erst ihren sicheren Boden. Zwei Wege zu diesem Ziele stehen uns offen. Der erste geht aus von den uns schon bekannten Nullpunkten der ϑ-Funktionen und setzt daraus unendliche Produkte zusammen.

Die Funktion $\vartheta_{00}(v)$ verschwindet nach § 21, wenn

$$2v = (2\nu - 1)\omega + (2\mu - 1)$$

ist, worin ν, μ ganze Zahlen sind, oder wenn

$$e^{\pm 2\pi i v} = -e^{\pi i\omega(2\nu - 1)},$$

worin wir nun ν auf positive Zahlen beschränken können. Setzen wir also zur Abkürzung

$$e^{\pi i\omega} = q,$$

so ist q eine Größe, deren absoluter Wert ein echter Bruch ist. Das konvergente unendliche Produkt

$$P(v) = \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1} e^{2\pi i v})(1 + q^{2\nu-1} e^{-2\pi i v})$$

verschwindet also in allen und nur in den Punkten, in denen $\vartheta_{00}(v)$ verschwindet, und es ist überdies

$$P(v+1) = P(v)$$
$$P(v+\omega) = \frac{1 + q^{-1} e^{-2\pi i v}}{1 + q e^{2\pi i v}} P(v) = q^{-1} e^{-2\pi i v} P(v).$$

Dies ist aber nach § 20, (1) die Periodeneigenschaft der Funktion $\vartheta_{00}(v)$, und wir haben daher:

$$(1) \qquad \vartheta_{00}(v) = Q \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1} e^{2\pi i v})(1 + q^{2\nu-1} e^{-2\pi i v}),$$

worin Q ein von v unabhängiger Faktor ist. Nach den Formeln (8) des § 21 erhält man hieraus, indem man v durch

$$v + \frac{1}{2}, \qquad v + \frac{\omega}{2}, \qquad v + \frac{1+\omega}{2}$$

ersetzt:

$$(2) \quad \vartheta_{01}(v) = Q \prod_{1,\infty}^{\nu} (1 - q^{2\nu-1} e^{2\pi i v})(1 - q^{2\nu-1} e^{-2\pi i v}),$$

$$(3) \quad \vartheta_{10}(v) = Q q^{\frac{1}{4}} (e^{\pi i v} + e^{-\pi i v}) \prod_{1,\infty}^{\nu} (1 + q^{2\nu} e^{2\pi i v})(1 + q^{2\nu} e^{-2\pi i v}),$$

$$(4) \quad \vartheta_{11}(v) = -i Q q^{\frac{1}{4}} (e^{\pi i v} - e^{-\pi i v}) \prod_{1,\infty}^{\nu} (1 - q^{2\nu} e^{2\pi i v})(1 - q^{2\nu} e^{-2\pi i v}).$$

Setzt man in diesen Formeln $v = 0$, in der letzten nach einmaliger Differentiation, so folgt

$$(5) \quad \begin{aligned} \vartheta_{00} &= Q \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1})^2, \\ \vartheta_{01} &= Q \prod_{1,\infty}^{\nu} (1 - q^{2\nu-1})^2, \\ \vartheta_{10} &= 2 Q q^{\frac{1}{4}} \prod_{1,\infty}^{\nu} (1 + q^{2\nu})^2, \\ \vartheta'_{11} &= 2\pi Q q^{\frac{1}{4}} \prod_{1,\infty}^{\nu} (1 - q^{2\nu})^2. \end{aligned}$$

Hiernach läßt sich mittels (5), § 23:

$$\vartheta'_{11} = \pi \vartheta_{00} \vartheta_{01} \vartheta_{10}$$

der Faktor Q bestimmen. Man erhält zunächst

$$1 = Q^2 \overset{\nu}{\Pi} \frac{(1 - q^{2\nu-1})^2 (1 + q^{2\nu-1})^2 (1 + q^{2\nu})^2}{(1 - q^{2\nu})^2},$$

oder, indem man über das noch unbestimmte Vorzeichen von Q und damit über die Vorzeichen der ϑ-Funktionen verfügt:

$$Q = \overset{\nu}{\underset{1,\infty}{\Pi}} \frac{(1 - q^{2\nu})}{(1 + q^{2\nu})(1 + q^{2\nu-1})(1 - q^{2\nu-1})}.$$

Im Nenner kann man für $\Pi(1 + q^{2\nu})(1 + q^{2\nu-1})$ setzen $\Pi(1 + q^{\nu})$, und der Zähler $\Pi(1 - q^{2\nu})$ läßt sich zerlegen in

$$\Pi(1 - q^{\nu})(1 + q^{\nu}) = \Pi(1 - q^{2\nu})(1 - q^{2\nu-1})(1 + q^{\nu}).$$

Dadurch ergibt sich endlich

(6) $$Q = \overset{\nu}{\Pi}(1 - q^{2\nu}).$$

Die Ausdrücke (1), (2), (3), (4) lassen sich in reeller Form darstellen, wenn man die Multiplikation der konjugiert imaginären Faktoren ausführt. Man erhält so:

(7)
$$\begin{aligned}
\vartheta_{00}(v) &= \overset{\nu}{\underset{1,\infty}{\Pi}}(1 - q^{2\nu})(1 + 2q^{2\nu-1}\cos 2\pi v + q^{4\nu-2}),\\
\vartheta_{01}(v) &= \overset{\nu}{\underset{1,\infty}{\Pi}}(1 - q^{2\nu})(1 - 2q^{2\nu-1}\cos 2\pi v + q^{4\nu-1}),\\
\vartheta_{10}(v) &= 2q^{\frac{1}{4}}\cos\pi v \overset{\nu}{\underset{1,\infty}{\Pi}}(1 - q^{2\nu})(1 + 2q^{2\nu}\cos 2\pi v + q^{4\nu}),\\
\vartheta_{11}(v) &= 2q^{\frac{1}{4}}\sin\pi v \overset{\nu}{\underset{1,\infty}{\Pi}}(1 - q^{2\nu})(1 - 2q^{2\nu}\cos 2\pi v + q^{4\nu}).
\end{aligned}$$

Führen wir den Ausdruck (6) in die letzte Gleichung (5) ein, so ergibt sich

$$\vartheta'_{11} = 2\pi q^{\frac{1}{4}} \Pi(1 - q^{2\nu})^3,$$

und wenn wir also

(8) $$\eta(\omega) = q^{\frac{1}{12}} \Pi(1 - q^{2\nu})$$

setzen, so wird

(9) $$\vartheta'_{11} = 2\pi\eta(\omega)^3.$$

Indem wir Q mit Hilfe der Relation

$$Q = q^{-\frac{1}{12}}\eta(\omega)$$

aus (5) eliminieren, setzen wir

(10)
$$\begin{aligned}
\vartheta_{00} &= \eta(\omega) f(\omega)^2,\\
\vartheta_{01} &= \eta(\omega) f_1(\omega)^2,\\
\vartheta_{10} &= \eta(\omega) f_2(\omega)^2,
\end{aligned}$$

worin die Funktionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ folgendermaßen definiert sind:

$$f(\omega) = q^{-\frac{1}{24}} \prod_{1,\infty}^{\nu} (1 + q^{2\nu-1}),$$

(11) $$f_1(\omega) = q^{-\frac{1}{24}} \prod_{1,\infty}^{\nu} (1 - q^{2\nu-1}),$$

$$f_2(\omega) = \sqrt{2}\, q^{\frac{1}{12}} \prod_{1,\infty}^{\nu} (1 + q^{2\nu}).$$

Die Funktionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ werden in unseren späteren Betrachtungen eine wichtige Rolle spielen. Aus § 21, (14) ergibt sich nach (10) die Relation

(12) $$f(\omega)^8 = f_1(\omega)^8 + f_2(\omega)^8,$$

und aus § 23 (5) nach (9)

(13) $$f(\omega) f_1(\omega) f_2(\omega) = \sqrt{2}.$$

Die letzte Formel ergibt sich auch aus (11) mit Benutzung der identischen Relation:

$$\Pi(1 + q^\nu)(1 - q^{2\nu-1}) = \Pi \frac{(1 + q^\nu)(1 - q^\nu)}{1 - q^{2\nu}} = 1.$$

§ 25. Darstellung der ϑ-Funktionen durch unendliche Reihen.

Der zweite Weg, um zur Darstellung der ϑ-Funktionen zu gelangen, besteht darin, daß man eine den Fundamentalgleichungen genügende konvergente unendliche Reihe zu bilden sucht.

Bemerken wir zunächst, daß wegen der Bedingung

$$\vartheta_{00}(v + 1) = \vartheta_{00}(v)$$

die Funktion $\vartheta_{00}(v)$ als eindeutige Funktion von $e^{2\pi i v}$ angesehen werden kann, und setzen demgemäß

$$\vartheta_{00}(v) = \sum_{-\infty,\infty}^{\nu} A_\nu e^{2\pi i v \nu},$$

so ergibt die Differentialgleichung § 20, (4):

$$\frac{\partial^2 \vartheta}{\partial v^2} - 4\pi i \frac{\partial \vartheta}{\partial \omega} = 0$$

für A_ν die Bedingung

$$\frac{dA_\nu}{d\omega} = \pi i \nu^2 A_\nu, \quad A_\nu = c_\nu e^{\pi i \omega \nu^2} = c_\nu q^{\nu^2},$$

worin c_ν in bezug auf ω konstant ist. Es wird also

$$\vartheta_{00}(v) = \Sigma c_\nu q^{\nu^2} e^{2\pi i v \nu},$$

und daraus:

$$\vartheta_{00}(v+\omega) = \Sigma\, c_\nu\, q^{\nu^2+2\nu}\, e^{2\pi i v \nu}$$
$$= q^{-1}\, e^{-2\pi i v}\, \Sigma\, c_\nu\, q^{(\nu+1)^2}\, e^{2\pi i v(\nu+1)}.$$

Da ν von $-\infty$ bis $+\infty$ geht, so ist es gestattet, in dieser Formel $\nu - 1$ an Stelle von ν zu setzen, und wenn man dies tut, so ergibt sich

$$\vartheta_{00}(v+\omega) = q^{-1}\, e^{-2\pi i v}\, \Sigma\, c_{\nu-1}\, q^{\nu^2}\, e^{2\pi i v \nu}.$$

Nach der zweiten der Fundamentalgleichungen [§ 20, (1)] müssen also die beiden Reihen

$$\Sigma\, c_\nu\, q^{\nu^2}\, e^{2\pi i v \nu} \quad \text{und} \quad \Sigma\, c_{\nu-1}\, q^{\nu^2}\, e^{2\pi i v \nu}$$

miteinander übereinstimmen, d. h. es muß

$$c_{\nu-1} = c_\nu$$

sein. Die c_ν sind also alle einander gleich; daß sie den Wert 1 haben, ergibt die Vergleichung der beiden Entwickelungen

$$\sum_{-\infty,\infty}^{\nu} q^{\nu^2}\, e^{2\pi i v \nu}, \quad \prod_{1,\infty}^{\nu} (1-q^{2\nu})(1+q^{2\nu-1}\, e^{2\pi i v})(1+q^{2\nu-1}\, e^{-2\pi i v})$$

für den Wert $q = 0$.

Der hiermit für $\vartheta_{00}(v)$ gefundenen Entwickelung kann man auch die beiden Formeln geben:

(1) $$\vartheta_{00}(v) = \Sigma\, q^{\nu^2}\, e^{2\nu\pi i v}$$
$$= 1 + 2q\cos 2\pi v + 2q^4\cos 4\pi v + 2q^9 \cos 6\pi v + \cdots,$$

und daraus erhält man nach § 21, (8) durch Vermehrung von v um $\frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$ die Entwickelungen für die drei übrigen ϑ-Funktionen:

(2) $$\vartheta_{01}(v) = \Sigma\,(-1)^\nu\, q^{\nu^2}\, e^{2\nu\pi i v}$$
$$= 1 - 2q\cos 2\pi v + 2q^4 \cos 4\pi v - 2q^9\cos 6\pi v + \cdots$$

(3) $$\vartheta_{10}(v) = \Sigma\, q^{\frac{(2\nu+1)^2}{4}}\, e^{(2\nu+1)\pi i v}$$
$$= 2q^{\frac{1}{4}}\cos \pi v + 2q^{\frac{9}{4}}\cos 3\pi v + 2q^{\frac{25}{4}}\cos 5\pi v + \cdots$$

(4) $$\vartheta_{11}(v) = -i\Sigma\,(-1)^\nu\, q^{\frac{(2\nu+1)^2}{4}}\, e^{(2\nu+1)\pi i v}$$
$$= 2q^{\frac{1}{4}}\sin \pi v - 2q^{\frac{9}{4}}\sin 3\pi v + 2q^{\frac{25}{4}}\sin 5\pi v + \cdots$$

Wir ziehen für spätere Anwendungen aus diesen Entwickelungen die Schlüsse:

Wenn der imaginäre Teil von ω ins Unendliche wächst, so daß der absolute Wert von q verschwindet, so wird

$$\vartheta_{00}(v) = 1, \quad \vartheta_{01}(v) = 1, \quad q^{-\frac{1}{4}}\vartheta_{10}(v) = 2\cos\pi v,$$
$$q^{-\frac{1}{4}}\vartheta_{11}(v) = 2\sin\pi v.$$

Nehmen wir ω rein imaginär, also q reell, positiv und echt gebrochen an, so sind für ein reelles v:

1. $\vartheta_{00}(v)$, $\vartheta_{01}(v)$, $\vartheta_{10}(v)$, $\vartheta_{11}(v)$ reell, und wenn v zwischen 0 und $\frac{1}{2}$ liegt, positiv [nach § 24 (7)], folglich auch ϑ_{00}, ϑ_{01}, ϑ_{10}, ϑ'_{11} positiv;

2. $\vartheta_{00}(iv)$, $\vartheta_{01}(iv)$, $\vartheta_{10}(iv)$, $-i\vartheta_{11}(iv)$ reell, und solange v zwischen 0 und $\dfrac{-i\omega}{2}$ liegt, positiv; ferner mit Zuziehung der Formeln § 21, (8)

3. $\vartheta_{00}(\frac{1}{2}+iv)$, $\vartheta_{01}(\frac{1}{2}+iv)$, $i\vartheta_{10}(\frac{1}{2}+iv)$, $\vartheta_{11}(\frac{1}{2}+iv)$ reell, und solange v zwischen 0 und $\dfrac{-i\omega}{2}$ liegt, positiv;

4. $$q^{\frac{1}{4}}e^{\pi i v}\vartheta_{00}\left(\frac{\omega}{2}+v\right), \quad -iq^{\frac{1}{4}}e^{\pi i v}\vartheta_{01}\left(\frac{\omega}{2}+v\right),$$
$$q^{\frac{1}{4}}e^{\pi i v}\vartheta_{10}\left(\frac{\omega}{2}+v\right), \quad -iq^{\frac{1}{4}}e^{\pi i v}\vartheta_{11}\left(\frac{\omega}{2}+v\right)$$
reell, und solange v zwischen 0 und $\frac{1}{2}$ liegt, positiv.

§ 26. Entwickelung von ϑ-Quotienten.

Bedeutet v eine Variable und a eine beliebige Konstante, so sind die Quotienten

$$\frac{\vartheta_{g_1, g_2}(v+a)}{\vartheta_{g'_1, g'_2}(v)}$$

doppeltperiodische Funktionen zweiter Art und erster Ordnung mit den Periodizitätsfaktoren $(-1)^{g_1+g'_1}$, $(-1)^{g_2+g'_2}e^{-2\pi i a}$, und wenn man einen Exponentialfaktor $e^{\lambda v}$ hinzufügt, so kann man λ und a so bestimmen, daß die Periodizitätsfaktoren beliebig gegebene Größen werden. Indem man die Hauptcharakteristiken (g_1, g_2), (g'_1, g'_2) auf alle mögliche Arten wählt, erhält man 16 solcher Funktionen. Wir gehen aus von einer unter ihnen, für die wir unter Hinzufügung eines konstanten Faktors

(1) $$F = \frac{\vartheta'_{11}\vartheta_{11}(v+a)}{2i\pi\vartheta_{11}(v)\vartheta_{11}(a)}$$

wählen. Dies ist eine eindeutige Funktion $F(z)$ der Variablen

$$z = e^{2\pi i v},$$

und wenn wie früher $q = e^{\pi i \omega}$ ist, so hat sie die Perioden-eigenschaft:

(2) $$F(q^2 z) = e^{-2\pi i a} F(z),$$

woraus für jedes ganzzahlige ν folgt:

$$F(q^{2\nu} z) = e^{-2\pi i a \nu} F(z).$$

Die Funktion $F(z)$ wird für ein endliches z nur dann unendlich, wenn einer der Faktoren $q^{2\nu} z - 1$ verschwindet, und es ist insbesondere

(3) $$(z - 1) F(z) = 1 \quad (\text{für } z = 1).$$

Nach (2) ist aber

$$(q^{2\nu} z - 1) F(q^{2\nu} z) = e^{-2\pi i a \nu} F(z) (q^{2\nu} z - 1)$$

und folglich ist nach (3)

(4) $$F(z)(q^{2\nu} z - 1) = e^{2\pi i a \nu} \quad (\text{für } z = q^{-2\nu}).$$

Setzen wir unter der gleich noch näher zu prüfenden Voraussetzung der Konvergenz

(5) $$S(z) = \sum_{-\infty,\infty}^{\nu} \frac{e^{2\pi i a \nu}}{q^{2\nu} z - 1},$$

so ergibt sich, indem wir z durch $q^2 z$ und ν durch $\nu - 1$ ersetzen:

(6) $$S(q^2 z) = e^{-2\pi i a} S(z),$$

und die Differenz $F(z) - S(z)$ wäre also, als Funktion von v betrachtet, nach (3) und (4) eine ganze doppeltperiodische Funktion zweiter Art. Eine solche muß aber nach § 16, 6. eine Exponentialfunktion sein, und es ist also

$$F(z) = S(z) + C e^{-2\pi i m v},$$

worin m eine ganze Zahl und C eine Konstante ist. Aus (2) und (6) aber ergibt sich, wenn nicht $C = 0$ ist:

$$e^{-2\pi i m \omega} = e^{-2\pi i a};$$

also $a = m\omega + n$, worin m, n ganze Zahlen sind. Ist aber a eine Periode, so reduziert sich $F(z)$ auf eine Konstante oder eine Exponentialfunktion. Anderenfalls muß $C = 0$ sein, und es folgt die Entwickelung:

(7) $$\frac{\vartheta_{11}' \vartheta_{11}(v + a)}{2 i\pi \vartheta_{11}(v) \vartheta_{11}(a)} = \sum_{-\infty,+\infty}^{\nu} \frac{e^{2\pi i \nu a}}{q^{2\nu} e^{2\pi i v} - 1}.$$

Wir haben die Konvergenz dieser Reihe für alle Werte von v vorausgesetzt; um diese zu beurteilen, bemerken wir, daß das allgemeine Glied dieser Reihe

$$\text{für } \nu = +\infty \text{ gleich } -e^{2\pi i\nu a}$$
$$\text{„ } \nu = -\infty \text{ „ } e^{-2\pi i v} e^{-2\pi i\nu(\omega-a)}$$

wird. Es wird also Konvergenz stattfinden, wenn der imaginäre Teil von a und von $\omega - a$ positiv ist. Setzen wir daher $\omega = \omega' + i\omega''$, $a = a' + ia''$, so ist die Bedingung der Konvergenz

$$0 < a'' < \omega''. \tag{8}$$

Wenn man in (7) a durch $a + \frac{1}{2}$ ersetzt, so ergibt sich die Entwickelung für eine zweite der 16 Funktionen:

$$\frac{\vartheta_{11}' \vartheta_{10}(v+a)}{2\pi i \vartheta_{11}(v) \vartheta_{10}(a)} = \sum^{\nu} \frac{(-1)^{\nu} e^{2\pi i a\nu}}{q^{2\nu} e^{2\pi i v} - 1}, \tag{9}$$

und wenn man in (7) und (9) a in $a + \frac{1}{2}\omega$ verwandelt:

$$\frac{\vartheta_{11}' \vartheta_{01}(v+a)}{2\pi i \vartheta_{11}(v) \vartheta_{01}(a)} = \sum^{\nu} \frac{e^{2\pi i a\nu} q^{\nu} e^{\pi i v}}{q^{2\nu} e^{2\pi i v} - 1}, \tag{10}$$

$$\frac{\vartheta_{11}' \vartheta_{00}(v+a)}{2\pi i \vartheta_{11}(v) \vartheta_{00}(a)} = \sum^{\nu} \frac{(-1)^{\nu} e^{2\pi i a\nu} q^{\nu} e^{\pi i v}}{q^{2\nu} e^{2\pi i v} - 1}, \tag{11}$$

wobei jedoch zu bemerken ist, daß in den letzten beiden Formeln die Konvergenzbedingung geändert ist, nämlich:

$$-\frac{\omega''}{2} < a'' < \frac{\omega''}{2}.$$

Aus den vier Formeln ergeben sich die übrigen zwölf, wenn wir v durch $v + \frac{1}{2}$, $v + \frac{1}{2}\omega$, $v + \frac{1}{2}(1 + \omega)$ ersetzen, wobei die Konvergenzbereiche nicht weiter geändert werden. Auf diese Weise sind die Formeln der Tabelle I am Schlusse des Bandes abgeleitet.

Die so gewonnenen Reihen konvergieren für reelle Werte von a nicht alle, z. B. tut es nicht die Reihe (7), worin der nach der Seite der positiven ν verlaufende Teil

$$\sum_{1,\infty}^{\nu} \frac{e^{2\pi i\nu a}}{q^{2\nu} e^{2\pi i v} - 1} \tag{12}$$

aufhört zu konvergieren, wenn der imaginäre Teil von a gleich Null wird, während der andere Teil auch da noch konvergent

bleibt. Man erhält aber aus (12) einen Ausdruck, der auch für ein reelles a noch konvergiert, wenn man die Summe

$$(13) \qquad \sum_{1,\infty}^{\nu} e^{2\pi i \nu a} = -\frac{e^{2\pi i a}}{e^{2\pi i a} - 1}$$

hinzufügt. Dadurch geht er nämlich über in

$$\sum_{1,\infty}^{\nu} \frac{e^{2\pi i \nu a}\, q^{2\nu}\, e^{2\pi i v}}{q^{2\nu}\, e^{2\pi i v} - 1},$$

und diese Reihe bleibt konvergent, solange der imaginäre Teil a'' von a zwischen $-\omega''$ und $+\omega''$ liegt.

Demnach ergibt sich aus (7), wenn wir das dem Werte $\nu = 0$ entsprechende Glied absondern und die negativen ν durch $-\nu$ ersetzen:

$$\frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{11}(a)} = \frac{2i}{e^{2\pi i v} - 1} + \frac{2 i e^{2\pi i a}}{e^{2\pi i a} - 1}$$
$$+ 2i \sum_{1,\infty}^{\nu} \frac{e^{-2\pi i \nu a}}{q^{-2\nu}\, e^{2\pi i v} - 1} + 2i \sum_{1,\infty}^{\nu} \frac{q^{2\nu}\, e^{2\pi i \nu a}\, e^{2\pi i v}}{q^{2\nu}\, e^{2\pi i v} - 1}.$$

Es ist aber

$$\frac{2i}{e^{2\pi i v} - 1} = \frac{e^{-\pi i v}}{\sin \pi v} = \operatorname{cotg} \pi v - i,$$
$$\frac{2 i e^{2\pi i a}}{e^{2\pi i a} - 1} = \frac{e^{\pi i a}}{\sin \pi a} = \operatorname{cotg} \pi a + i,$$

und demnach läßt sich diese Entwickelung auch so darstellen:

$$(14) \qquad \begin{aligned} \frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{11}(a)} &= \operatorname{cotg} \pi v + \operatorname{cotg} \pi a \\ &- 2i \sum \left(\frac{q^m\, e^{m\pi i a}}{e^{-2\pi i v} - q^m} - \frac{q^m\, e^{-m\pi i a}}{e^{2\pi i v} - q^m}\right), \end{aligned}$$

worin m die Reihe der geraden Zahlen

$$m = 2, 4, 6, 8, \ldots$$

durchläuft. Der Gültigkeitsbereich dieser Entwickelung ist

$$-\omega'' < a'' < \omega''.$$

In der Tabelle II sind diese 16 Entwickelungen zusammengestellt.

Aus diesen Formeln sind drei andere ableitbar, indem man v oder a oder beide um $\frac{1}{2}$ vermehrt. Drei andere aber, die der Vermehrung von v und a um $\frac{1}{2}\omega$ entsprechen, müssen direkt abgeleitet werden. Sie zeigen reelle Form, wenn q, a, v reell sind.

Eine dritte Art der Entwickelung, in der die Symmetrie der Funktionen in bezug auf die beiden Variablen v, a zum Ausdruck kommt, ergibt sich, wenn man die Brüche, die in den vorigen Entwickelungen auftraten, nach Potenzen von q entwickelt. So erhält man

$$\frac{q^m}{e^{-2\pi i v} - q^m} = \Sigma q^{m\nu} e^{2\pi i \nu v},$$

$$\frac{q^m}{e^{+2\pi i v} - q^m} = \Sigma q^{m\nu} e^{-2\pi i \nu v},$$

$$\nu = 1, 2, 3, \ldots$$

und diese Entwickelungen gelten, solange der absolute Wert von $q\, e^{2\pi i v}$ ein echter Bruch ist, also, wenn $v = v' + i v''$ gesetzt wird, solange

$$-\omega'' < v < \omega''$$

ist. Hiernach ergibt sich aus (14)

$$\frac{\vartheta'_{11}\, \vartheta_{11}(v+a)}{\pi\, \vartheta_{11}(v)\, \vartheta_{11}(a)} = \operatorname{cotg} \pi v + \operatorname{cotg} \pi a$$

$$+ 4\, \Sigma\, q^{\frac{m m'}{2}} \sin(m a + m' v)\pi,$$

worin m, m' voneinander unabhängig die geraden Zahlen 2, 4, 6, 8, ... durchlaufen. Diese Formel ist gültig für reelle a und v und gilt darüber hinaus noch, solange der imaginäre Teil, sowohl von v als von a, absolut kleiner ist als ω''.

In der Tabelle III sind die 16 Formeln dieser Art zusammengestellt [1]).

[1]) Solche Entwickelungen sind von Jacobi (sur la rotation d'un corps) (ges. Werke Bd. II), hierauf von Hermite (Annales de l'école normale 1885) und von Kronecker (Berliner Akademie 1885) betrachtet. Vgl. auch die Straßburger Dissertation von L. Vockerodt (1905).

Dritter Abschnitt.

Transformation der Theta-Funktionen.

---

§ 27. Das Transformationsprinzip.

Wir kehren zurück zu den in § 17 gegebenen Definitionsgleichungen der T-Funktionen $m$ter Ordnung und versehen darin aus einem gleich ersichtlichen Grunde die Buchstaben ω, a, b, m mit Akzenten, so daß diese Gleichungen lauten:

$$(1)\qquad \begin{aligned} T(u + \omega_1') &= e^{-\pi i [a'_1(2u+\omega'_1)+b'_1]}\, T(u), \\ T(u + \omega_2') &= e^{-\pi i [a'_2(2u+\omega'_2)+b'_2]}\, T(u). \end{aligned}$$

$$(2)\qquad a_2'\omega_1' - a_1'\omega_2' = m'.$$

Sind a, c irgend welche ganze (positive oder negative) Zahlen, so ergibt sich, wenn man in § 17, (16) n_1, n_2 durch $-c$, a ersetzt:

$$(3)\qquad \begin{aligned} &T(u - c\omega_1' + a\omega_2') \\ &= e^{-\pi i(-c a'_1 + a a'_2)(2u - c\omega'_1 + a\omega'_2) - \pi i(-c b'_1 + a b'_2 - m' a c)}\, T(u), \end{aligned}$$

eine Gleichung, die auch aus einer der Gleichungen (1) hervorgeht, wenn man darin a', b', ω' durch

$$-ca_1' + aa_2', \qquad -cb_1' + ab_2' - m'ac, \qquad -c\omega_1' + a\omega_2'$$

ersetzt.

Hierin ist das Prinzip der Transformation der T-Funktionen enthalten.

Es seien b, ∂ zwei andere ganze Zahlen, für welche die Determinante

$$(4)\qquad n = a\partial - bc$$

einen positiven Wert hat. Wir setzen

$$(5)\qquad \begin{aligned} \omega_1 &= +\partial\omega_1' - b\omega_2', \\ \omega_2 &= -c\omega_1' + a\omega_2', \end{aligned}$$

und folglich

$$(6)\qquad \begin{aligned} n\omega_1' &= a\omega_1 + b\omega_2 \\ n\omega_2' &= c\omega_1 + \partial\omega_2. \end{aligned}$$

Es hat dann, wie man aus

$$\frac{\omega_2'}{\omega_1'} = \frac{c\,\omega_1 + \partial\,\omega_2}{a\,\omega_1 + b\,\omega_2}$$

durch Trennung des reellen vom imaginären Teil erkennt, der imaginäre Teil von $\omega_2 : \omega_1$ dasselbe Vorzeichen, wie der von $\omega_2' : \omega_1'$ (das positive).

Setzen wir

$$(7) \qquad \begin{aligned} a_1 &= \partial a_1' - b a_2' \\ a_2 &= -c a_1' + a a_2' \end{aligned}$$

$$(8) \qquad \begin{aligned} b_1 &= \partial b_1' - b b_2' - m' b \partial \\ b_2 &= -c b_1' + a b_2' - m' a c, \end{aligned}$$

so schließt man aus (3), daß die Funktion $T(u)$ nicht nur den Bedingungen (1), sondern auch den aus (1) durch Vertauschung von ω_1', ω_2', a_1', a_2', b_1', b_2' mit ω_1, ω_2, a_1, a_2, b_1, b_2 hervorgehenden Gleichungen, d. h. den Gleichungen (1), § 17, genügt. Sie ist also gleichzeitig eine T-Funktion der Perioden ω_1', ω_2' und der Perioden ω_1, ω_2, was wir durch folgende Gleichung andeuten:

$$(9) \qquad T'(u, \omega_1' \omega_2') = T(u, \omega_1, \omega_2).$$

Es ist aber nach (5) und (7)

$$a_2\,\omega_1 - a_1\,\omega_2 = (a_2'\,\omega_1' - a_1'\,\omega_2')(a\partial - bc),$$

also, wenn m die Ordnung von T ist,

$$(10) \qquad m = m'n.$$

Nach (8) ist die Charakteristik (g_1, g_2) von T, wenn (g_1', g_2') die von T' ist (§ 17),

$$(11) \quad (g_1, g_2) = (\partial g_1' - b g_2' - m' b \partial, \; -c g_1' + a g_2' - m' a c).$$

Unter der Transformation der T-Funktionen versteht man die Darstellung der Funktionen T' mit den Perioden ω_1', ω_2' durch T-Funktionen mit den Perioden ω_1, ω_2.

Die Zahlen a, b, c, ∂ heißen die Transformationszahlen und $n = a\partial - bc$ der Transformationsgrad.

Um die Form dieser Darstellung deutlicher zu übersehen, wollen wir die Bedingungen aufsuchen, unter denen $T(u, \omega_1, \omega_2)$ eine Θ-Funktion der $m$ten Ordnung $\Theta(u, \omega)$ wird (§ 20). Wir nehmen b_1', b_2' und folglich auch b_1, b_2 als ganze Zahlen, so daß b_1, b_2, b_1', b_2' durch g_1, g_2, g_1', g_2' ersetzt werden können. Es ist dann

$$\omega_1 = 1, \qquad \omega_2 = \omega, \qquad a_1 = 0, \qquad a_2 = m$$

zu setzen, und demnach wird [nach (6), (7), (10)]

$$\omega_1' = \frac{a + b\,\omega}{n}, \qquad \omega_2' = \frac{c + \partial\,\omega}{n},$$
$$a_1' = m'b, \qquad a_2' = m'\partial.$$

Die Funktion $T'(u, \omega_1', \omega_2')$ genügt also den Bedingungen (1):

$$T(u + \omega_1') = (-1)^{g'_1} e^{-\pi i m' b (2u + \omega'_1)} T(u),$$
$$T(u + \omega_2') = (-1)^{g'_2} e^{-\pi i m' \partial (2u + \omega'_2)} T(u),$$

und daraus ergibt sich, daß das Produkt

$$e^{\frac{\pi i m' b u^2}{\omega'_1}} T'(u, \omega_1', \omega_2')$$

eine Θ-Funktion der Ordnung m' ist, mit den Argumenten

$$\frac{u}{\omega_1'}, \quad \frac{\omega_2'}{\omega_1'}$$

und der Charakteristik (g_1', g_2'). Wir können dies in der Gleichung ausdrücken:

$$(12) \qquad e^{-\frac{\pi i m' n b u^2}{a + b\omega}} \Theta^{(m')}_{g'_1, g'_2}\left(\frac{nu}{a + b\omega}, \frac{c + \partial\omega}{a + b\omega}\right) = \Theta^{(m'n)}_{g_1, g_2}(u, \omega),$$

worin die Charakteristiken durch (11) bestimmt sind. Die Mittel zur Darstellung dieser Funktionen sind in § 21 enthalten.

Wir bezeichnen die Transformation von T und T' durch einen einzelnen Buchstaben S oder durch (T', T), also:

$$S = (T', T).$$

Bedeutet S' eine zweite Transformation, durch die T' in T'' übergeht, also

$$S' = (T'', T'),$$

so können wir daraus eine neue Transformation S'' ableiten, durch die T in T'' übergeht. Diese heißt aus S und S' zusammengesetzt und wird so bezeichnet:

$$S'' = S'S$$

oder

$$(T'', T) = (T'', T')(T', T).$$

Bei dieser Zusammensetzung gilt im allgemeinen nicht das kommutative Gesetz; es ist also SS' von $S'S$ verschieden. Es gilt aber das assoziative Gesetz, das sich in der Formel ausspricht:

$$(T''', T'')[(T'', T')(T', T)] = [(T''', T'')(T'', T')](T', T) = (T''', T).$$

§ 28. Zusammensetzung der Transformationen.

Eine Transformation [§ 27, (9)] ist vollständig bestimmt durch die Transformationszahlen a, b, c, ∂, und diese vier ganzen Zahlen können beliebig gegeben sein, wenn nur ihre Determinante $n = a\partial - bc$ positiv ist. Gibt man diesen vier Zahlen das entgegengesetzte Zeichen, so gehen ω_1', ω_2' nach § 27, (6) in $-\omega_1'$, $-\omega_2'$ über, und ersetzt man a, b, c, d durch ma, mb, mc, $m\partial$, worin m eine beliebige natürliche Zahl ist, so gehen ω_1', ω_2' in ω_1'/m, ω_2'/m und n in $m^2 n$ über. Das Periodenverhältnis $\omega' = \omega_2'/\omega_1'$ bleibt in diesen beiden Fällen ungeändert. Einstweilen wollen wir aber zwei Transformationen immer als verschieden betrachten, wenn die Transformationszahlen verschieden sind. Nach dieser Festsetzung können wir eine Transformation unzweideutig durch eine Matrix

$$(1) \qquad S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

darstellen. Die Determinante

$$(2) \qquad n = a\partial - bc$$

ist der Transformationsgrad.

Nach dieser Bezeichnung stellen wir die Relationen (6), § 27 auch so dar:

$$(3) \qquad n(\omega_1', \omega_2') = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}(\omega_1, \omega_2).$$

Setzt man

$$S' = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix}, \quad a'\partial' - b'c' = n',$$

so ist

$$(4) \qquad n'(\omega_1'', \omega_2'') = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix}(\omega_1', \omega_2'),$$

und wenn man in (4) ω_1', ω_2' nach (3) durch ω_1, ω_2 ausdrückt, so erhält man

$$(5) \qquad nn'(\omega_1'', \omega_2'') = \begin{pmatrix} a'a + b'c, & a'b + b'\partial \\ c'a + \partial'c, & c'b + \partial'\partial \end{pmatrix}(\omega_1, \omega_2).$$

Setzen wir also

$$(6) \qquad S'' = S'S,$$

so ist

$$S'' = \begin{pmatrix} a'a + b'c, & a'b + b'\partial \\ c'a + \partial'c, & c'b + \partial'\partial \end{pmatrix} = \begin{pmatrix} a'', & b'' \\ c'', & \partial'' \end{pmatrix},$$

$$a''\partial'' - b''c'' = n'' = nn'.$$

Die Transformationen S setzen sich also nach derselben Regel zusammen wie die linearen Substitutionen und Matrizes, die wir im sechsten Abschnitte des zweiten Bandes betrachtet haben. Der Grad einer zusammengesetzten Transformation ist gleich dem Produkte der Grade der Komponenten. Diese Matrizes sind hier an die Voraussetzung gebunden, daß ihre Elemente ganze Zahlen und ihre Determinante positiv ist.

Diese Eigenschaften bleiben bei der Zusammensetzung der Transformationen erhalten. Trotzdem bildet die Gesamtheit $\mathfrak{S}$ der Transformationen S keine Gruppe, so wenig wie die Gesamtheit der natürlichen Zahlen bei der Komposition durch Multiplikation eine Gruppe ist; denn es läßt sich bei gegebenem S', S'' nicht immer ein S bestimmen, das der Bedingung (6) genügt, was doch (nach Bd. II, § 1, 4.) für eine Gruppe erforderlich wäre.

Durch die spezielle Transformation vom Grade m^2:

$$M = \begin{pmatrix} \pm m, & 0 \\ 0, & \pm m \end{pmatrix}$$

gehen die Perioden ω_1, ω_2 in $\omega_1' = \omega_1/m$, $\omega_2' = \omega_2/m$ über, und das Periodenverhältnis $\omega = \omega_2/\omega_1$ bleibt ungeändert. Diese Transformationen heißen M u l t i p l i k a t i o n e n (Ähnlichkeits-Transformationen, Bd. II, § 41). Es ist darunter die identische Substitution

$$1 = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$$

enthalten, die alles ungeändert läßt und bei der Komposition die Rolle der Einheit spielt.

Die Multiplikationen sind bei der Zusammensetzung mit jeder Transformation S vertauschbar:

$$(7) \qquad SM = MS.$$

Hält man in SM oder MS die Transformation S fest und läßt M die Gesamtheit $\mathfrak{M}$ der Multiplikationen durchlaufen, so erhält man ein System $\mathfrak{M}S$, das man nach Bd. II, § 46 als eine Kollineation zu bezeichnen hätte. Gehören S_1 und S_2 einer Kollineation C an und S_1' und S_2' einer Kollineation C', so gehören auch $S_1'S_1$ und $S_2'S_2$ derselben Kollineation C'' an. Man kann so, indem man $C'' = C'C$ setzt, die Kollineationen zusammensetzen. Bei dieser Zusammensetzung spielt die Kolli-

neation $\mathfrak{M}$ die Rolle der Einheit. Ist $S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ eine beliebige Transformation, so ist

$$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} \begin{pmatrix} \partial, & -b \\ -c, & a \end{pmatrix} = \begin{pmatrix} n, & 0 \\ 0, & n \end{pmatrix}$$

eine Multiplikation. Die beiden Kollineationen

$$C = \mathfrak{M} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \quad C^{-1} = \mathfrak{M} \begin{pmatrix} \partial, & -b \\ -c, & a \end{pmatrix}$$

geben also bei der Komposition $CC^{-1} = C^{-1}C = \mathfrak{M}$ und sind also zueinander reziprok.

Demnach bildet die Gesamtheit der Kollineationen eine Gruppe.

Die Transformationen vom Grade 1 heißen lineare Transformationen. Wir bezeichnen bei diesen die Transformationszahlen zum Unterschiede mit den griechischen Buchstaben $\alpha, \beta, \gamma, \delta$, so daß

$$L = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \alpha\delta - \beta\gamma = 1$$

eine lineare Transformation bedeutet. Das System $\mathfrak{L}$ der linearen Transformationen ist eine in $\mathfrak{S}$ enthaltene Gruppe, denn sind

$$L = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad L' = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix},$$

so ist

$$L'' = L'L = \begin{pmatrix} \alpha'\alpha + \beta'\gamma, & \alpha'\beta + \beta'\delta \\ \gamma'\alpha + \delta'\gamma, & \gamma'\beta + \delta'\delta \end{pmatrix} = \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix}$$

gleichfalls linear, und man kann L bei gegebenem L', L'' aus den Gleichungen

$$\alpha'\alpha + \beta'\gamma = \alpha'', \quad \alpha'\beta + \beta'\delta = \beta'',$$
$$\gamma'\alpha + \delta'\gamma = \gamma'', \quad \gamma'\beta + \delta'\delta = \delta''$$

eindeutig bestimmen. Die Einheit der Gruppe $\mathfrak{L}$ ist die identische Substitution $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ und jede Substitution L hat ihre Reziproke L^{-1}, wie aus der Zusammensetzung

$$LL^{-1} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \delta, & -\beta \\ -\gamma, & \alpha \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$$

hervorgeht. Die Gruppe $\mathfrak{L}$ ist unendlich und ist nicht kommutativ.

Aus der Gleichung

$$(8) \qquad \alpha\delta - \beta\gamma = 1$$

folgt, daß weder α, β noch α, γ, noch δ, β, noch δ, γ einen gemeinschaftlichen Faktor haben können. Hat man aber α, β beliebig ohne gemeinschaftlichen Teiler angenommen, so kann man γ, δ noch auf unendlich viele Arten aus (8) bestimmen. Ist γ, δ eine dieser Bestimmungen, so sind sie alle in der Form

$$(9) \qquad \gamma + \lambda\alpha, \qquad \delta + \lambda\beta$$

enthalten, worin λ eine beliebige ganze Zahl ist (Bd. I, § 126).

§ 29. Zusammensetzung der Transformationen aus einfacheren.

In dem System $\mathfrak{S}$ aller Transformationen S ist ein System $\mathfrak{S}_0$ enthalten, das aus allen den Transformationen S_0 besteht, deren zweite Transformationszahl $b = 0$ ist, während a und ∂ positiv sind:

$$(1) \qquad S_0 = \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}.$$

Bei der Zusammensetzung zweier S_0 entsteht wieder ein S_0, aber doch ist $\mathfrak{S}_0$ so wenig eine Gruppe wie $\mathfrak{S}$.

Man kann jede beliebige Transformation

$$S = \begin{pmatrix} p, & q \\ r, & s \end{pmatrix}$$

durch eine Zusammensetzung LS auf ein S_0 zurückführen. Soll nämlich

$$(2) \qquad \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}\begin{pmatrix} p, & q \\ r, & s \end{pmatrix} = \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}$$

sein, so muß α, β der Bedingung genügen:

$$\alpha q + \beta s = 0,$$

und wenn also ∂ der größte gemeinschaftliche Teiler von q und s ist, so setze man

$$\partial\alpha = s, \qquad \partial\beta = -q,$$

und bestimme, nachdem α und β hierdurch als relative Primzahlen ermittelt sind, γ und δ aus der Formel (8), § 28. Dann ist (2) erfüllt, wenn

$$a\partial = n, \qquad c = \gamma p + \delta r$$

gesetzt wird; a und ∂ sind hierdurch eindeutig bestimmt, c kann aber bei anderer Wahl von γ und δ durch $c + \lambda a$ ersetzt werden. Man kann daher über λ so verfügen, daß c in der Reihe

der Zahlen 0, 1, 2 ... $a - 1$ enthalten ist, und dadurch ist dann die Substitution S_0 vollständig bestimmt.

Wenn die vier Transformationszahlen einen gemeinsamen Faktor haben, so läßt sich dieser mittels der Formel

$$\begin{pmatrix} m, & 0 \\ 0, & m \end{pmatrix} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} ma, & mb \\ mc, & m\partial \end{pmatrix}$$

durch Zusammensetzung mit der Multiplikation absondern, und wir setzen demnach jetzt voraus, daß a, b, c, ∂ keinen gemeinschaftlichen Teiler haben. Man kann dann immer die zwei ganzen Zahlen ξ, η so bestimmen, daß

$$(3) \qquad \begin{aligned} a\eta - c\xi &= \alpha \\ b\eta - \partial\xi &= \beta \end{aligned}$$

ohne gemeinsamen Teiler sind.

Um dies einzusehen, setzen wir zunächst ξ, η relativ prim voraus. Dann ist jeder gemeinsame Teiler von α, β notwendig Teiler von n, wie man aus den Auflösungen von (3)

$$(4) \qquad \begin{aligned} n\xi &= b\alpha - a\beta \\ n\eta &= \partial\alpha - c\beta \end{aligned}$$

erkennt. Nimmt man also ξ nicht teilbar durch alle in a und b zugleich aufgehenden Primzahlen, dagegen ξ teilbar, η unteilbar durch alle anderen in n aufgehenden Primzahlen, und überdies ξ, η relativ prim, was stets möglich ist, so haben α und β keinen gemeinsamen Teiler. Hierauf bestimmt man γ, δ so, daß

$$\alpha\delta - \beta\gamma = 1.$$

Es ist dann nach (3) auch

$$(a\delta - b\gamma)\eta - (c\delta - \partial\gamma)\xi = 1,$$

und es ergibt sich die folgende Zusammensetzung, wie leicht mit Benutzung von (4) erkannt wird:

$$(5) \qquad \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \begin{pmatrix} a\delta - b\gamma, & \xi \\ c\delta - \partial\gamma, & \eta \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix} \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}.$$

Nennen wir also

$$(6) \qquad \begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}$$

die Haupttransformation vom Grade n, so ist damit bewiesen, daß sich alle Transformationen vom Grade n aus einer Multiplikation, einer Haupttransformation und linearen Transformationen zusammensetzen lassen.

Aus der Zusammensetzung

(7) $$\begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}1, & 0\\ 0, & m\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & mn\end{pmatrix}, \quad \begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}n, & 0\\ 0, & 1\end{pmatrix} = \begin{pmatrix}n, & 0\\ 0, & n\end{pmatrix}$$

können wir noch weiter schließen, daß sich jede Transformation vom Grade n aus solchen zusammensetzen läßt, deren Grad eine Primzahl ist. Zerlegt man $n = pq$ in zwei Faktoren p und q, die zueinander relativ prim sind, so ergibt sich, indem man die Zahlen β, δ aus

$$p\delta - q\beta = 1$$

bestimmt, die Zusammensetzung

$$\begin{pmatrix}p, & \beta\\ q, & \delta\end{pmatrix}\begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}p\delta, & -q\beta\\ -1, & 1\end{pmatrix} = \begin{pmatrix}p, & 0\\ 0, & q\end{pmatrix},$$

woraus zu ersehen ist, daß man statt der Haupttransformation auch jede dieser Transformationen $\begin{pmatrix}p, & 0\\ 0, & q\end{pmatrix}$ zur Ableitung aller anderen benutzen kann.

§ 30. Die linearen Fundamentaltransformationen.

Die ganze Gruppe $\mathfrak{L}$ der linearen Transformationen läßt sich durch Wiederholung von zweien unter ihnen, die wir die linearen Fundamentaltransformationen nennen, ableiten.

Ist

$$L = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \qquad \alpha\delta - \beta\gamma = 1$$

eine beliebige lineare Transformation, so ist

(1) $$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix},$$

und da die identische Transformation die Einheit in der Gruppe L ist, so ist

$$L^{-1} = \begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$$

die zu L reziproke Transformation.

Wir bezeichnen durch die Potenz $L^{\pm m}$ das, was durch $m$malige Wiederholung von L oder L^{-1} entsteht, und wollen nun nachweisen, daß sich durch die Potenzen der Fundamentaltransformationen

(2) $$A = \begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}, \quad B = \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$$

jede Substitution L der Gruppe $\mathfrak{L}$ zusammensetzen läßt. Es ist zunächst

$$(3) \qquad A^{-1} = \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix}, \quad A^{\lambda} = \begin{pmatrix} 1, & 0 \\ \lambda, & 1 \end{pmatrix}$$

(für jedes ganzzahlige positive oder negative λ)

$$(4) \qquad B^{-1} = \begin{pmatrix} 0, & -1 \\ 1, & 0, \end{pmatrix}, \quad B^2 = \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}, \quad B^3 = B^{-1}.$$

Wir setzen noch

$$(5) \qquad C = \begin{pmatrix} 1, & -1 \\ 0, & 1 \end{pmatrix} = B^{-1} A B, \quad C^{\lambda} = \begin{pmatrix} 1, & -\lambda \\ 0, & 1 \end{pmatrix},$$

C ist also aus A und B ableitbar.

Nun sei $L = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ eine beliebige lineare Transformation. Wir leiten daraus die Reihe ab:

$$L' = L A^{\lambda}, \quad L'' = L' C^{\lambda'}, \quad L''' = L'' A^{\lambda''}, \quad L'''' = L''' C^{\lambda'''},$$

deren erste und zweite Elemente so gebildet sind:

$$\alpha' = \alpha + \lambda \beta, \quad \beta'' = \beta' - \lambda' \alpha', \quad \alpha''' = \alpha'' + \lambda'' \beta'',$$
$$\beta'''' = \beta''' - \lambda''' \alpha''', \ldots,$$

und man kann über $\lambda, \lambda', \lambda'', \lambda''', \ldots$ so verfügen, daß, dem absoluten Werte nach

$$\alpha' \leqq \tfrac{1}{2} \beta, \quad \beta'' \leqq \tfrac{1}{2} \alpha', \quad \alpha''' \leqq \tfrac{1}{2} \beta'', \quad \beta'''' \lesseqgtr \tfrac{1}{2} \alpha''' \ldots,$$

solange keine dieser Zahlen verschwindet. Die Zahlen

$$\beta, \alpha', \beta'', \alpha''', \beta'''', \ldots$$

bilden daher eine dem absoluten Werte nach abnehmende Zahlenreihe, und nach einer endlichen Anzahl von Zusammensetzungen dieser Art muß eine Zahl dieser Reihe verschwinden.

Ist $\beta^{(\nu)} = 0$, so ist

$$L^{(\nu)} = \begin{pmatrix} \pm 1, & 0 \\ \gamma^{(\nu)}, & \pm 1 \end{pmatrix} = \begin{pmatrix} \pm 1, & 0 \\ 0, & \pm 1 \end{pmatrix} A^{\pm \gamma^{(\nu)}}$$

und ist $\alpha^{(\nu)} = 0$, so ist

$$L^{(\nu)} = \begin{pmatrix} 0, & \pm 1 \\ \mp 1, & \delta^{(\nu)} \end{pmatrix} = A^{\pm \delta^{\nu}} B^{\mp 1},$$

und da

$$L = L' A^{-\lambda} = L'' C^{-\lambda'} A^{-\lambda}$$
$$= L''' A^{-\lambda''} C^{-\lambda'} A^{-\lambda} = L'''' C^{-\lambda'''} A^{-\lambda''} C^{-\lambda'} A^{-\lambda}, \ldots$$

ist, so ist der Satz bewiesen.

§ 31. Die linearen Fundamentaltransformationen der ϑ-Funktionen.

Bei der Anwendung auf die Transformation der Θ-Funktionen [§ 27, (12)] kommt zunächst der transformierte Modul

$$\omega' = \frac{c + \partial\omega}{a + b\omega}$$

in Betracht. Dieser ändert sich nicht, wenn die vier Transformationszahlen einen gemeinsamen Faktor m bekommen. Die Transformation heißt eine **eigentliche**, wenn a, b, c, ∂ keinen gemeinsamen Faktor haben.

Das transformierte Argument

$$u' = \frac{nu}{a + b\omega}$$

geht über in mu', wenn a, b, c, ∂ durch $ma, mb, mc, m\partial$, also n durch $m^2 n$ ersetzt wird. Die Multiplikation $\begin{pmatrix} m, & 0 \\ 0, & m \end{pmatrix}$ läßt den Modul ω ungeändert und verwandelt u in mu.

Nach den Resultaten der beiden vorigen Paragraphen läßt sich das ganze System der eigentlichen Transformationen herleiten durch wiederholte Anwendung der drei Transformationen

$$\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad \begin{pmatrix} n, & 0 \\ 0, & 1 \end{pmatrix},$$

und wir betrachten also zunächst die linearen Fundamentaltransformationen der ϑ-Funktionen.

I. $\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$ oder $(\omega, \omega + 1)$.

Nach § 27, (11), (12) ist

(1) $$\vartheta_{11}(u, \omega + 1) = A\vartheta_{11}(u, \omega),$$

worin A von u unabhängig ist. Ersetzt man u durch

$$u + \frac{1}{2}, \quad u + \frac{\omega}{2}, \quad u + \frac{1 + \omega}{2},$$

so ergeben die Formeln § 21, (8)

(2) $$\vartheta_{10}(u, \omega + 1) = A\vartheta_{10}(u, \omega)$$

(3) $$e^{\frac{\pi i}{4}}\vartheta_{00}(u, \omega + 1) = A\vartheta_{01}(u, \omega)$$

(4) $$e^{\frac{\pi i}{4}}\vartheta_{01}(u, \omega + 1) = A\vartheta_{00}(u, \omega).$$

Zur Bestimmung der Konstanten A wenden wir, wie in der Folge häufig, das Mittel an, daß wir $u = 0$ setzen, in (1) nach der Differentiation, und dann rechts und links von der Formel (5), § 23

$$(5) \qquad \vartheta'_{11} = \pi \vartheta_{00} \vartheta_{10} \vartheta_{01}$$

Gebrauch machen; so folgt

$$A^2 = e^{\frac{\pi i}{2}}, \quad A = e^{\frac{\pi i}{4}};$$

daß bei A das positive Zeichen steht, ergibt sich aus einer der Formeln (3), (4) nach der Schlußbemerkung von § 25, wenn man ω unendlich werden läßt.

Sonach erhält man

$$(6) \qquad \begin{aligned} \vartheta_{11}(u, \omega + 1) &= e^{\frac{\pi i}{4}} \vartheta_{11}(u) \\ \vartheta_{10}(u, \omega + 1) &= e^{\frac{\pi i}{4}} \vartheta_{10}(u) \\ \vartheta_{01}(u, \omega + 1) &= \vartheta_{00}(u) \\ \vartheta_{00}(u, \omega + 1) &= \vartheta_{01}(u). \end{aligned}$$

II. $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$ oder $\left(\omega, \frac{-1}{\omega}\right)$.

Es ist wieder nach § 27, (12)

$$(7) \qquad e^{-\frac{\pi i u^2}{\omega}} \vartheta_{11}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = A \vartheta_{11}(u, \omega),$$

und durch Vermehrung von u um $\frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$

$$(8) \qquad e^{-\frac{\pi i u^2}{\omega}} \vartheta_{01}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A \vartheta_{10}(u, \omega),$$

$$(9) \qquad e^{-\frac{\pi i u^2}{\omega}} \vartheta_{10}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A \vartheta_{01}(u, \omega),$$

$$(10) \qquad e^{-\frac{\pi i u^2}{\omega}} \vartheta_{00}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) = i A \vartheta_{00}(u, \omega),$$

woraus man wie oben erhält:

$$A = \pm i \sqrt{-i\omega}.$$

Aus $u = 0$ und einem rein imaginären ω schließt man, daß, wenn $\sqrt{-i\omega}$ so genommen wird, daß der reelle Teil positiv ist, das untere Zeichen stehen muß, und es ergibt sich daher:

$$
(11)\qquad
\begin{aligned}
e^{-\frac{\pi i u^2}{\omega}}\vartheta_{11}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= -i\sqrt{-i\omega}\,\vartheta_{11}(u),\\
e^{-\frac{\pi i u^2}{\omega}}\vartheta_{01}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\,\vartheta_{10}(u),\\
e^{-\frac{\pi i u^2}{\omega}}\vartheta_{10}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\,\vartheta_{01}(u),\\
e^{-\frac{\pi i u^2}{\omega}}\vartheta_{00}\left(\frac{u}{\omega}, -\frac{1}{\omega}\right) &= \sqrt{-i\omega}\,\vartheta_{00}(u).
\end{aligned}
$$

§ 32. Die Haupttransformationen zweiter Ordnung der ϑ-Funktionen.

Die beiden Haupttransformationen $n$ter Ordnung

$$\begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix},\qquad \begin{pmatrix}n, & 0\\ 0, & 1\end{pmatrix}$$

verwandeln nach § 27, (11) die Charakteristik (g_1, g_2) in

$$(ng_1, g_2),\quad (g_1, ng_2),$$

d. h. bei ungeradem n bleibt die Charakteristik ungeändert, bei geradem n geht sie über in

$$(1)\qquad (0, g_2) \text{ oder } (g_1, 0).$$

Da sich hiernach die Transformation geraden Grades wesentlich anders verhält als die ungeraden Grades, so betrachten wir zunächst den Fall $n = 2$. Die erste und zweite Haupttransformation zweiten Grades werden die Landensche und die Gausssche Transformation genannt.

Nach § 27, (12) sind

$$
(2)\qquad
\begin{aligned}
\vartheta_{g_1, g_2}\left(u, \frac{\omega}{2}\right) &= \Theta_{g_1, 0}(u, \omega)\\
\vartheta_{g_1, g_2}(2u, 2\omega) &= \Theta_{0, g_2}(u, \omega)
\end{aligned}
$$

Θ-Funktionen zweiter Ordnung von u, ω, die sich nach § 21 darstellen lassen.

Wir erhalten zunächst die zwei Formelpaare, in denen A, B von u unabhängig sind:

$$
(3)\qquad
\begin{aligned}
A\vartheta_{11}\left(u, \frac{\omega}{2}\right) &= \vartheta_{01}(u, \omega)\,\vartheta_{11}(u, \omega),\\
A\vartheta_{10}\left(u, \frac{\omega}{2}\right) &= \vartheta_{00}(u, \omega)\,\vartheta_{10}(u, \omega),
\end{aligned}
$$

$$
(4)\qquad
\begin{aligned}
B\vartheta_{11}(2u, 2\omega) &= \vartheta_{10}(u, \omega)\,\vartheta_{11}(u, \omega),\\
B\vartheta_{01}(2u, 2\omega) &= \vartheta_{00}(u, \omega)\,\vartheta_{01}(u, \omega),
\end{aligned}
$$

wovon jedesmal die zweite aus der ersten abgeleitet werden kann durch Vermehrung des Arguments um eine halbe Periode.

Setzt man in diesen Gleichungen $u = 0$, so folgt

$$(5\quad \begin{aligned} A\vartheta'_{11}\left(0, \frac{\omega}{2}\right) &= \vartheta_{01}\vartheta'_{11}, \quad 2B\vartheta'_{11}(0, 2\omega) = \vartheta_{10}\vartheta'_{11}, \\ A\vartheta_{10}\left(0, \frac{\omega}{2}\right) &= \vartheta_{00}\vartheta_{10}, \quad B\vartheta_{01}(0, 2\omega) = \vartheta_{00}\vartheta_{01}, \end{aligned}$$

woraus durch Division, mit Benutzung der Relation

$$\vartheta'_{11} = \pi\vartheta_{00}\vartheta_{11}\vartheta_{01},$$

$$(6)\qquad \vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{01}\left(0, \frac{\omega}{2}\right) = \vartheta_{01}^2,$$

$$(7)\qquad 2\vartheta_{00}(0, 2\omega)\vartheta_{10}(0, 2\omega) = \vartheta_{10}^2,$$

und wenn man in (6) ω durch 2ω, in (7) ω durch $\omega:2$ ersetzt:

$$(8)\qquad \vartheta_{01}(0, 2\omega)^2 = \vartheta_{00}\vartheta_{01},$$

$$(9)\qquad \vartheta_{10}\left(0, \frac{\omega}{2}\right)^2 = 2\vartheta_{00}\vartheta_{10}.$$

Nach (8) und (9) ergibt sich aus den zweiten Gleichungen (5):

$$2A = \vartheta_{10}\left(0, \frac{\omega}{2}\right), \quad B = \vartheta_{01}(0, 2\omega),$$

und man erhält also für die Gausssche Transformation:

$$(10)\quad \begin{aligned} \vartheta_{10}\left(0, \frac{\omega}{2}\right)\vartheta_{11}\left(u, \frac{\omega}{2}\right) &= 2\vartheta_{01}(u, \omega)\vartheta_{11}(u, \omega), \\ \vartheta_{10}\left(0, \frac{\omega}{2}\right)\vartheta_{10}\left(u, \frac{\omega}{2}\right) &= 2\vartheta_{00}(u, \omega)\vartheta_{10}(u, \omega), \end{aligned}$$

und für die Landensche Transformation:

$$(11)\quad \begin{aligned} \vartheta_{01}(0, 2\omega)\vartheta_{11}(2u, 2\omega) &= \vartheta_{10}(u, \omega)\vartheta_{11}(u, \omega), \\ \vartheta_{01}(0, 2\omega)\vartheta_{01}(2u, 2\omega) &= \vartheta_{00}(u, \omega)\vartheta_{01}(u, \omega). \end{aligned}$$

Es bleiben für jede der beiden Transformationen noch zwei ϑ-Funktionen auszudrücken. Man kann diese Ausdrücke aus (10), (11) herleiten nach § 21, (13), gelangt aber auch direkt dazu auf folgende Weise. Die Funktionen

$$(12)\qquad \vartheta_{01}\left(u, \frac{\omega}{2}\right), \quad \vartheta_{10}(2u, 2\omega)$$

verschwinden für

$$u = \frac{\omega}{4}, \quad u = \frac{1}{4}.$$

Andererseits ergibt sich aus den Formeln (8) des § 21, wenn dort $v = -\frac{\omega}{4}$ und $= -\frac{1}{4}$ gesetzt wird,

$$\vartheta_{11}\left(\frac{\omega}{4}\right) = i\,\vartheta_{01}\left(\frac{\omega}{4}\right)$$

$$\vartheta_{11}\left(\frac{1}{4}\right) = \vartheta_{10}\left(\frac{1}{4}\right)$$

und demnach sind die beiden Funktionen (12), die linear durch zwei ϑ-Quadrate ausdrückbar sind, von konstanten Faktoren abgesehen, übereinstimmend mit

$$\vartheta_{01}^2(u) + \vartheta_{11}^2(u), \quad \vartheta_{10}^2(u) - \vartheta_{11}^2(u).$$

Die konstanten Faktoren ergeben sich unmittelbar durch $u = 0$ aus den Relationen (6), (7):

$$\vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{01}\left(u, \frac{\omega}{2}\right) = \vartheta_{01}^2(u) + \vartheta_{11}^2(u), \tag{13}$$

$$2\,\vartheta_{00}(0, 2\,\omega)\,\vartheta_{10}(2\,u, 2\,\omega) = \vartheta_{10}^2(u) - \vartheta_{11}^2(u). \tag{14}$$

Daraus erhält man die beiden letzten Formeln, wenn man u in $u + \frac{1}{2}$ und $u + \frac{\omega}{2}$ verwandelt [oder auch auf demselben Wege wie (13), (14)]:

$$\vartheta_{00}\left(0, \frac{\omega}{2}\right)\vartheta_{00}\left(u, \frac{\omega}{2}\right) = \vartheta_{00}^2(u) + \vartheta_{10}^2(u), \tag{15}$$

$$2\,\vartheta_{00}(0, 2\,\omega)\,\vartheta_{00}(2\,u, 2\,\omega) = \vartheta_{00}^2(u) + \vartheta_{01}^2(u). \tag{16}$$

Hieraus lassen sich mannigfache Relationen zwischen den Nullwerten der ϑ-Funktionen herleiten, von denen wir nur die drei folgenden anführen, deren beide ersten aus (8), (9) fließen, während sich die letzte aus der ersten Gleichung (11) ergibt, wenn man ω durch $\omega : 2$ ersetzt und $u = {}^1/_4$ annimmt und berücksichtigt, daß $\vartheta_{11}({}^1/_4) = \vartheta_{10}({}^1/_4)$ ist.

$$\begin{aligned} \sqrt{\vartheta_{00}\,\vartheta_{01}} &= \vartheta_{01}(0, 2\,\omega), \\ \sqrt{\vartheta_{00}\,\vartheta_{10}} &= \frac{1}{\sqrt{2}}\,\vartheta_{10}\left(0, \frac{\omega}{2}\right), \\ \sqrt{\vartheta_{01}\,\vartheta_{10}} &= \vartheta_{10}\left(\frac{1}{4}, \frac{\omega}{2}\right). \end{aligned} \tag{17}$$

Diese Formeln sind darum von Interesse, weil sie die Quadratwurzeln als eindeutige Funktionen von ω darstellen.

Wir machen von der Transformation zweiter Ordnung noch eine Anwendung auf den Beweis einer Formel, die für die Transformation ungerader Ordnung notwendig ist.

Wir ersetzen in der zweiten Gleichung (10) ω durch $2\,\omega$, also:

$$2\,\vartheta_{00}(u,\,2\,\omega)\,\vartheta_{10}(u,\,2\,\omega) = \vartheta_{10}\,\vartheta_{10}(u).$$

Hiermit multiplizieren wir die zweite Gleichung (11), so daß wir erhalten

$$2\,\vartheta_{01}(0,\,2\,\omega)\,\vartheta_{01}(2\,u,\,2\,\omega)\,\vartheta_{00}(u,\,2\,\omega)\,\vartheta_{10}(u,\,2\,\omega) \\ = \vartheta_{10}\,\vartheta_{10}(u)\,\vartheta_{00}(u)\,\vartheta_{01}(u).$$

Dies dividieren wir durch das Produkt der beiden Gleichungen (7), (8):

$$2\,\vartheta_{00}(0,\,2\,\omega)\,\vartheta_{10}(0,\,2\,\omega)\,\vartheta_{01}(0,\,2\,\omega)^2 = \vartheta_{10}^2\,\vartheta_{00}\,\vartheta_{01}$$

und erhalten

$$(18)\quad \frac{\vartheta_{00}(u,\,2\,\omega)\,\vartheta_{10}(u,\,2\,\omega)\,\vartheta_{01}(2\,u,\,2\,\omega)}{\vartheta_{00}(0,\,2\,\omega)\,\vartheta_{10}(0,\,2\,\omega)\,\vartheta_{01}(0,\,2\,\omega)} = \frac{\vartheta_{00}(u)\,\vartheta_{10}(u)\,\vartheta_{01}(u)}{\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}}.$$

Wenn nun n irgend eine ungerade ganze Zahl bedeutet, so bleibt die Funktion

$$\vartheta_{01}\left(\frac{\nu}{n}\right),$$

wenn ν um ein Vielfaches von n wächst, ungeändert, und folglich ist das Produkt

$$\overset{\nu}{\Pi}\,\vartheta_{01}\left(\frac{\nu}{n}\right),$$

wenn es über ein volles Restsystem nach dem Modul n genommen wird, unabhängig von der besonderen Wahl dieses Restsystems. Daher ist, da $2\,\nu$ zugleich mit ν ein solches Restsystem durchläuft,

$$(19)\quad \overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{01}\left(\frac{\nu}{n}\right) = \overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{01}\left(\frac{2\,\nu}{n}\right).$$

Wenn wir also in (18) $u = \nu : n$ setzen, das Produkt bilden und im letzten Faktor der linken Seite von der Formel (19) Gebrauch machen, so ergibt sich, daß das Produkt

$$(20)\quad \frac{\overset{\nu}{\underset{1,\,n-1}{\Pi}}\,\vartheta_{00}\left(\frac{\nu}{n}\right)\,\vartheta_{10}\left(\frac{\nu}{n}\right)\,\vartheta_{01}\left(\frac{\nu}{n}\right)}{\vartheta_{00}^{n-1}\,\vartheta_{10}^{n-1}\,\vartheta_{01}^{n-1}}$$

ungeändert bleibt, wenn ω durch $2\,\omega$ ersetzt wird.

Die in (20) vorkommenden Werte von v lassen sich in Paare anordnen derart:

$$v,\ n - v, \qquad v = 1, 2, \dots \frac{n-1}{2},$$

und da

$$\vartheta_{00}\left(\frac{v}{n}\right) = \vartheta_{00}\left(\frac{n-v}{n}\right), \quad \vartheta_{10}\left(\frac{v}{n}\right) = -\vartheta_{10}\left(\frac{n-v}{n}\right),$$

$$\vartheta_{01}\left(\frac{v}{n}\right) = \vartheta_{01}\left(\frac{n-v}{n}\right),$$

so stimmt (20) bis auf das Vorzeichen überein mit dem Quadrat von

$$(21) \qquad \frac{\prod\limits_{1, \frac{n-1}{2}}^{v} \vartheta_{00}\left(\frac{v}{n}\right) \vartheta_{10}\left(\frac{v}{n}\right) \vartheta_{01}\left(\frac{v}{n}\right)}{\vartheta_{00}^{\frac{n-1}{2}}\ \vartheta_{10}^{\frac{n-1}{2}}\ \vartheta_{01}^{\frac{n-1}{2}}}.$$

Der letzte Quotient, der eine stetige, von Null verschiedene Funktion von ω ist, solange der imaginäre Teil von ω positiv ist, bleibt also gleichfalls ungeändert, wenn ω durch 2ω, also auch durch 4ω, 8ω, ... ersetzt wird. Man kann den Wert dieses Ausdruckes dadurch bestimmen, daß man den imaginären Teil von ω unendlich, also $q = 0$ annimmt. Für $q = 0$ ist aber (nach § 25):

$$\vartheta_{00}(v) = 1, \quad \vartheta_{01}(v) = 1, \quad \frac{\vartheta_{10}(v)}{\vartheta_{10}} = \cos \pi v,$$

und daher der Wert von (21):

$$(22) \qquad \prod_{1, \frac{n-1}{2}}^{v} \cos \frac{v\pi}{n}.$$

Da hierin $v\pi/n$ kleiner als $\frac{1}{2}\pi$ ist, so hat dieses Produkt einen positiven Wert. Es ist aber

$$\cos \frac{v\pi}{n} = -\cos \frac{(n-v)\pi}{n}$$

und nach Bd. I, § 144 ist

$$2^{\frac{n-1}{2}} \prod_{1, \frac{n-1}{2}}^{v} \cos \frac{v\pi}{n} = 1.$$

Dadurch ist die Formel bewiesen:

$$(23) \quad 2^{\frac{n-1}{2}} \prod_{1, \frac{n-1}{2}}^{v} \vartheta_{00}\left(\frac{v}{n}\right) \vartheta_{10}\left(\frac{v}{n}\right) \vartheta_{01}\left(\frac{v}{n}\right) = \vartheta_{00}^{\frac{n-1}{2}}\ \vartheta_{10}^{\frac{n-1}{2}}\ \vartheta_{01}^{\frac{n-1}{2}}.$$

Mit Rücksicht auf die Formel Bd. I, § 145, (3) kann man dieser Relation noch die Form geben:

$$(24)\quad 2^{\frac{n-1}{2}} \prod_{1,\frac{n-1}{2}} \vartheta_{00}\left(\frac{2\nu}{n}\right) \vartheta_{10}\left(\frac{2\nu}{n}\right) \vartheta_{01}\left(\frac{2\nu}{n}\right) = (-1)^{\frac{n^2-1}{8}} \vartheta_{00}^{\frac{n-1}{2}} \vartheta_{10}^{\frac{n-1}{2}} \vartheta_{01}^{\frac{n-1}{2}}.$$

§ 33. Die Haupttransformationen ungerader Ordnung.

Die zuletzt bewiesene Formel ist uns von Nutzen bei der Durchführung der Transformation ungerader Ordnung n. Wir betrachten zunächst die erste Haupttransformation. Nach § 27, (12) ist

$$(1)\qquad \vartheta_{11}(nu, n\omega)$$

eine Θ_{11}-Funktion $n$ter Ordnung von u und ω, und diese läßt sich aus ihren Nullpunkten leicht bilden, deren es im Periodenparallelogramm n gibt. Die Nullpunkte von (1) sind die Werte

$$u = \frac{\nu + \mu n \omega}{n} = \frac{\nu}{n} + \mu\omega,$$

wenn ν und μ ganze Zahlen sind, und man erhält alle inkongruenten unter diesen Werten, wenn man μ festhält und ν ein volles Restsystem nach dem Modul n durchlaufen läßt. Wir wählen das Restsystem

$$0, \pm 1, \pm 2, \ldots, \pm\frac{(n-1)}{2},$$

und erhalten demnach, wenn C einen von u unabhängigen Faktor bedeutet,

$$(2)\quad C\vartheta_{11}(nu, n\omega) = \vartheta_{11}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{\nu}{n} + u\right) \vartheta_{11}\left(\frac{\nu}{n} - u\right),$$

eine Formel, die sich nach § 22, (4) in folgender Weise auch durch die Funktionen $\vartheta_{11}(u)$, $\vartheta_{01}(u)$ ausdrücken läßt:

$$C\vartheta_{01}^{n-1}\vartheta_{11}(nu, n\omega) = \vartheta_{11}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \left[\vartheta_{11}^2\left(\frac{\nu}{n}\right)\vartheta_{01}^2(u) - \vartheta_{01}^2\left(\frac{\nu}{n}\right)\vartheta_{11}^2(u)\right].$$

Wir ersetzen u durch

$$u + \frac{1}{2}, \quad u + \frac{\omega}{2}, \quad u + \frac{1+\omega}{2}$$

und erhalten aus (8) (§ 21):

$$C\vartheta_{10}(nu,\, n\omega) = \vartheta_{10}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{10}\left(\frac{\nu}{n}+u\right)\vartheta_{10}\left(\frac{\nu}{n}-u\right),$$

$$(3)\qquad C\vartheta_{01}(nu,\, n\omega) = \vartheta_{01}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{01}\left(\frac{\nu}{n}+u\right)\vartheta_{01}\left(\frac{\nu}{n}-u\right),$$

$$C\vartheta_{00}(nu,\, n\omega) = \vartheta_{00}(u) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{00}\left(\frac{\nu}{n}+u\right)\vartheta_{00}\left(\frac{\nu}{n}-u\right).$$

Daraus aber ergibt sich für $u = 0$ nach der Formel $\vartheta'_{11} = \pi\vartheta_{00}\vartheta_{01}\vartheta_{10}$:

$$4)\qquad C\prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{\nu}{n}\right) = \sqrt{n}\prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{00}\left(\frac{\nu}{n}\right)\vartheta_{01}\left(\frac{\nu}{n}\right)\vartheta_{01}\left(\frac{\nu}{n}\right),$$

oder mit Benutzung von (23) des vorigen Paragraphen:

$$(5)\qquad C\,2^{\frac{n-1}{2}}\prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{\nu}{n}\right) = \sqrt{n}\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}.$$

Das Vorzeichen ergibt sich aus dem Umstande, der aus einer der Formeln (3) folgt, daß $C = 1$ wird für $q = 0$.

Nach dieser Bestimmung von C lassen sich die Formeln (2), (3) so schreiben:

$$(6)\qquad \begin{aligned}&\sqrt{n}\,\vartheta_{11}(nu,\, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}\\ &= 2^{\frac{n-1}{2}}\vartheta_{11}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{\nu}{n}\right)\vartheta_{11}\left(\frac{\nu}{n}+u\right)\vartheta_{11}\left(\frac{\nu}{n}-u\right).\end{aligned}$$

$$(7)\qquad \begin{aligned}&\sqrt{n}\,\vartheta_{10}(nu,\, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}\\ &= 2^{\frac{n-1}{2}}\vartheta_{10}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{\nu}{n}\right)\vartheta_{01}\left(\frac{\nu}{n}+u\right)\vartheta_{01}\left(\frac{\nu}{n}-u\right).\end{aligned}$$

$$(8)\qquad \begin{aligned}&\sqrt{n}\,\vartheta_{01}(nu,\, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}\\ &= 2^{\frac{n-1}{2}}\vartheta_{01}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{\nu}{n}\right)\vartheta_{01}\left(\frac{\nu}{n}+u\right)\vartheta_{01}\left(\frac{\nu}{n}-u\right).\end{aligned}$$

$$(9)\qquad \begin{aligned}&\sqrt{n}\,\vartheta_{00}(nu,\, n\omega)\,\vartheta_{00}^{\frac{n-1}{2}}\,\vartheta_{10}^{\frac{n-1}{2}}\,\vartheta_{01}^{\frac{n-1}{2}}\\ &= 2^{\frac{n-1}{2}}\vartheta_{00}(u)\prod_{1,\frac{n-1}{2}}^{\nu}\vartheta_{11}\left(\frac{\nu}{n}\right)\vartheta_{00}\left(\frac{\nu}{n}+u\right)\vartheta_{00}\left(\frac{\nu}{n}-u\right).\end{aligned}$$

§ 34. Die Funktionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$.

Es sind bereits im § 24 die Funktionen $\eta(\omega)$, $f(\omega)$, $f_1($ $f_2(\omega)$ erwähnt, die sich dort als einwertige Funktionen von bei der Darstellung der ϑ-Funktionen durch unendliche Produk fast von selbst einstellten, die sich aber nicht ergaben bei d zweiten Darstellung durch unendliche Reihen. Damit im Z sammenhange steht ein bemerkenswerter Umstand, daß vie unserer Formeln, z. B. die zur Transformation zweiter Ordnu gehörigen (17), § 32 oder die Formel (23), § 32, leicht verifizie werden können durch die unendlichen Produkte, dagegen schw oder gar nicht durch die unendlichen Reihen. Darum war es fi uns von Interesse, diese Resultate ohne die Benutzung des ein oder anderen dieser Ausdrücke aus der Transformationstheor herzuleiten, und ebenso sollen nun auch aus dieser Quelle d Funktionen $\eta(\omega)$, $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ und ihre Grundeigenschafte gewonnen werden.

Die Formel (6) des vorigen Paragraphen ergibt für $n =$
$\sqrt{3}\,\vartheta_{11}(3u, 3\omega)\vartheta_{00}\vartheta_{10}\vartheta_{01} = 2\vartheta_{11}(\frac{1}{3})\vartheta_{11}(u)\vartheta_{11}(\frac{1}{3}+u)\vartheta_{11}(\frac{1}{3}-u$
und wenn man differentiiert und dann $u = 0$ setzt nach (4):

$$3\sqrt{3}\,\vartheta'_{11}(0, 3\omega) = 2\pi\vartheta_{11}(\tfrac{1}{3})^3,$$

oder indem man ω durch $\frac{\omega}{3}$ ersetzt,

$$3\sqrt{3}\,\vartheta'_{11} = 2\pi\left[\vartheta_{11}\left(\frac{1}{3}, \frac{\omega}{3}\right)\right]^3.$$

Setzt man also

(1) $$\eta(\omega) = \frac{1}{\sqrt{3}}\vartheta_{11}\left(\frac{1}{3}, \frac{\omega}{3}\right),$$

so folgt in der Bezeichnung übereinstimmend mit § 24 (9):

(2) $$\vartheta'_{11} = \pi\vartheta_{00}\vartheta_{01}\vartheta_{10} = 2\pi\eta(\omega)^3$$

und aus § 25, (4) erhält man für $\eta(\omega)$ die Reihenentwickelun

(3) $$\eta(\omega) = q^{\frac{1}{12}}\sum_{-\infty,\infty}^{\nu}(-1)^{\nu}q^{3\nu^2+\nu}.$$

Die Funktion $\eta(\omega)$ ist für ein rein imaginäres ω (reelles q reell, und für ein unendlich großes ω (d. h. verschwindendes q) ist

$$q^{-\frac{1}{12}}\eta(\omega) = 1.$$

Hiernach findet man, wenn man in (2) die Formeln § 31, (6), (11) anwendet, für die linearen Fundamentaltransformationen von $\eta(\omega)$

(4)
$$\eta(\omega+1) = e^{\frac{\pi i}{12}}\eta(\omega),$$

(5)
$$\eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\,\eta(\omega),$$

von denen die erste auch unmittelbar aus der Reihendarstellung (3) folgt, während die zweite nicht so leicht durch direkte Umformung der Reihen bewiesen werden kann.

Wir gehen über zur Betrachtung der beiden Haupttransformationen zweiter Ordnung der η-Funktion.

Aus § 32, (11) erhält man durch Differentiation und Nullsetzen von u

$$2\,\vartheta_{01}(0, 2\omega)\,\eta(2\omega)^3 = \vartheta_{10}\,\eta(\omega)^3,$$

also wenn man ins Quadrat erhebt und § 32, (8) anwendet:

$$4\,\vartheta_{00}\,\vartheta_{10}\,\vartheta_{01}\,\eta(2\omega)^6 = \vartheta_{10}^3\,\eta(\omega)^6,$$

und mit Anwendung von (2) und Ausziehen der Kubikwurzel:

(6)
$$2\,\eta(2\omega)^2 = \vartheta_{10}\,\eta(\omega).$$

Ersetzt man in (6) ω durch $\frac{\omega}{2}$, so folgt

$$2\,\eta(\omega)^2 = \vartheta_{10}\left(0, \frac{\omega}{2}\right)\eta\left(\frac{\omega}{2}\right),$$

und wenn man quadriert und die Formel § 32 (9) anwendet:

$$2\,\eta(\omega)^4 = \eta\left(\frac{\omega}{2}\right)^2 \vartheta_{00}\,\vartheta_{10}.$$

Multipliziert man beiderseits mit ϑ_{01}, so folgt nach (2):

(7)
$$\eta\left(\frac{\omega}{2}\right)^2 = \vartheta_{01}\,\eta(\omega)$$

und durch Verwandlung von ω in $\omega+1$ [(4) und § 31, (6)]:

(8)
$$e^{-\frac{\pi i}{12}}\eta\left(\frac{\omega+1}{2}\right)^2 = \vartheta_{00}\,\eta(\omega).$$

Hiernach führen wir die drei Funktionen ein:

$$f(\omega) = \frac{e^{-\frac{\pi i}{24}} \eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)},$$

(9) $$f_1(\omega) = \frac{\eta\left(\frac{\omega}{2}\right)}{\eta(\omega)},$$

$$f_2(\omega) = \sqrt{2}\,\frac{\eta(2\omega)}{\eta(\omega)}.$$

Dann ist nach (6), (7), (8)

(10) $$\vartheta_{00} = \eta(\omega) f(\omega)^2, \quad \vartheta_{01} = \eta(\omega) f_1(\omega)^2, \quad \vartheta_{10} = \eta(\omega) f_2(\omega)^2,$$

und aus (8) und (9) folgt, daß $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ für ein rein imaginäres ω reell und positiv sind. (10) stimmt überein mit § 24, (10), und die dort eingeführten Funktionen f, f_1, f_2 sind dieselben wie diese. Aus (10) folgen aber leicht die Relationen [(2) und § 21 (14)]:

(11) $$f(\omega)^8 = f_1(\omega)^8 + f_2(\omega)^8, \quad \sqrt{2} = f(\omega) f_1(\omega) f_2(\omega).$$

Mit Hilfe dieser Formeln kann man durch Quadratwurzeln jede der drei Funktionen $f(\omega)^8$, $f_1(\omega)^8$, $f_2(\omega)^8$ durch jede andere ausdrücken. Dazu führt die aus (11) fließende Formel:

(12) $$[f_1(\omega)^8 - f_2(\omega)^8]^2 = f(\omega)^{16} - \frac{64}{f(\omega)^8},$$
$$[f(\omega)^8 + f_2(\omega)^8]^2 = f_1(\omega)^{16} + \frac{64}{f_1(\omega)^8},$$
$$[f(\omega)^8 + f_1(\omega)^8]^2 = f_2(\omega)^{16} + \frac{64}{f_2(\omega)^8}.$$

Für die linearen Fundamentaltransformationen der Funktionen f erhält man zunächst aus (4) und (9):

(13) $$f(\omega+1) = e^{-\frac{\pi i}{24}} f_1(\omega),$$
$$f_1(\omega+1) = e^{-\frac{\pi i}{24}} f(\omega),$$
$$f_2(\omega+1) = e^{\frac{\pi i}{12}} f_2(\omega).$$

Ferner ergibt sich aus (5) und den beiden letzten Gleichungen (9):

$$(14)\qquad f_1\left(-\frac{1}{\omega}\right) = f_2(\omega), \qquad f_2\left(-\frac{1}{\omega}\right) = f_1(\omega),$$

und wenn man hiervon in der zweiten Gleichung (11) Gebrauch macht:

$$(15)\qquad f\left(-\frac{1}{\omega}\right) = f(\omega).$$

Für die Transformation zweiter Ordnung folgt unmittelbar aus den beiden letzten Gleichungen (9):

$$(16)\qquad f_1(2\,\omega) f_2(\omega) = \sqrt{2},$$

woraus sich noch durch Anwendung von (12) ergibt:

$$(17)\qquad f_2(\omega)^4 [f(2\,\omega)^8 + f_2(2\,\omega)^8] = 2\,[f(\omega)^8 + f_1(\omega)^8].$$

Setzt man in (16) nach (13), (14)

$$f_1(2\,\omega) = e^{-\frac{\pi i}{24}} f(2\,\omega - 1),$$
$$f_2(\omega) = e^{\frac{\pi i}{24}} f\left(1 - \frac{1}{\omega}\right),$$

so ergibt sich:

$$f\left(1 - \frac{1}{\omega}\right) f(2\,\omega - 1) = \sqrt{2},$$

und indem man $2\,\omega - 1$ gleich einem neuen ω setzt:

$$(18)\qquad f(\omega) f\left(\frac{\omega - 1}{\omega + 1}\right) = \sqrt{2}.$$

Ersetzt man in (16) ω durch $\frac{\omega}{2}$ und $\frac{\omega + 1}{2}$, so folgt:

$$(19)\qquad \begin{aligned} f_1(\omega) f_2\left(\frac{\omega}{2}\right) &= \sqrt{2}, \\ f(\omega) f_2\left(\frac{\omega + 1}{2}\right) &= e^{\frac{\pi i}{24}} \sqrt{2}. \end{aligned}$$

Wir stellen endlich noch für ein ungerades n die Formeln für die Haupttransformation $n$ter Ordnung der Funktionen η, f auf. Für $\eta(n\,\omega)$ ergibt sich leicht, wenn man in den Formeln (6), § 33 nach der Differentiation $u = 0$ setzt, und die dritte Wurzel zieht:

$$(20)\qquad \sqrt{n}\,\eta(n\,\omega)\,\eta(\omega)^{\frac{n-3}{2}} = \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{11}\left(\frac{\nu}{n}\right).$$

Setzt man ferner $u = 0$ in (7), (8), (9), § 33, benutzt alsdann die Relationen (10) und (20) und zieht die Quadratwurzel, so findet sich

$$\begin{aligned} f(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} &= f(\omega) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{00}\left(\frac{\nu}{n}\right), \\ f_1(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} &= f_1(\omega) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{01}\left(\frac{\nu}{n}\right), \qquad (21) \\ f_2(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} &= f_2(\omega) \prod_{1,\frac{n-1}{2}}^{\nu} \vartheta_{10}\left(\frac{\nu}{n}\right). \end{aligned}$$

Die Vorzeichen ergeben sich hier aus der Annahme eines unendlich kleinen q.

§ 35. Die Weierstrasssche σ-Funktion.

Durch die allgemeine lineare Substitution

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \quad \alpha\delta - \beta\gamma = 1,$$

angewandt auf die Variablen ω_1, ω_2, geht jede t-Funktion wieder in eine t-Funktion über, wobei die Charakteristik sich geändert hat. Ist (g_1, g_2) die Charakteristik der ursprünglichen, (g_1', g_2') die der transformierten Funktion, so ist nach § 27, (11)

$$(g_1, g_2) = (\delta g_1' - \beta g_2' - \beta\delta, \; -\gamma g_1' + \alpha g_2' - \alpha\gamma).$$

Löst man die beiden darin enthaltenen linearen Gleichungen für g_1', g_2' auf und beachtet, daß $\alpha\beta(\gamma + \delta + 1)$, $\gamma\delta(\alpha + \beta + 1)$ notwendig gerade Zahlen sind, und daß eine Charakteristik sich nicht ändert, wenn sich ihre Elemente um Vielfache von 2 ändern, so kann man dafür auch setzen:

$$(g_1', g_2') = (\alpha g_1 + \beta g_2 + \alpha\beta, \; \gamma g_1 + \delta g_2 + \gamma\delta). \qquad (1)$$

Die ϑ-Funktionen gehen also, abgesehen von Exponentialfaktoren, ineinander über. Von Wichtigkeit ist es aber, eine Funktion zu bilden, die den linearen Transformationen gegenüber absolut invariant ist, und eine solche Funktion ist die von Weierstrass in die Theorie eingeführte σ-Funktion, zu deren Definition wir jetzt übergehen.

Wenn wir die Formel (1) auf die vier Hauptcharakteristiken (0, 0), (0, 1), (1, 0), (1, 1) anwenden, so gehen diese der Reihe

nach über in $(\alpha\beta, \gamma\delta)$, $[(\alpha+1)\beta, (\gamma+1)\delta]$, $[\alpha(\beta+1), \gamma(\delta+1)]$, $[(\alpha+1)(\beta+1)-1, (\gamma+1)(\delta+1)-1) = (1, 1)]$. Es bleibt also nur die letzte Charakteristik (1, 1) bei allen linearen Transformationen ungeändert, da weder α und β noch γ und δ zugleich gerade Zahlen sein können. Es sei also $t(u, \omega_1, \omega_2)$ eine t-Funktion von der Charakteristik (1, 1), die nach § 17, (12) für $u = 0$ verschwinden muß.

Ist
$$(\omega_1', \omega_2') = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(\omega_1, \omega_2),$$
so sind nach unserem Transformationsprinzip
$$t(u, \omega_1, \omega_2) \quad \text{und} \quad t(u, \omega_1', \omega_2')$$
verwandte T-Funktionen erster Ordnung, und folglich ist, wenn C, λ, μ von u unabhängige Größen sind,

$$t(u, \omega_1', \omega_2') = Ce^{\lambda u^2 + \mu u}\, t(u, \omega_1, \omega_2). \tag{2}$$

Es ergibt sich hieraus durch logarithmische Differentiation

$$2\lambda u + \mu = \frac{d\log t(u, \omega_1', \omega_2')}{du} - \frac{d\log t(u, \omega_1, \omega_2)}{du}. \tag{3}$$

Nun ist, wenn wir nach Potenzen von u nach dem Taylorschen Lehrsatz entwickeln und mit t', t'', t''' die erste, zweite, dritte Derivierte von t nach u für $u = 0$ bezeichnen,

$$\frac{d\log t(u, \omega_1, \omega_2)}{du} = \frac{1}{u} + \frac{t''}{2t'} + u\left(\frac{t'''}{3t'} - \frac{t''^2}{4t'^2}\right) + \cdots,$$

woraus sich durch Vergleichung mit (3) ergibt, daß λ und μ in die Form gesetzt werden können:

$$\lambda = \varphi(\omega_1', \omega_2') - \varphi(\omega_1, \omega_2),$$
$$\mu = \psi(\omega_1', \omega_2') - \psi(\omega_1, \omega_2),$$

worin

$$\varphi(\omega_1, \omega_2) = \frac{t'''}{6t'} - \frac{t''^2}{8t'^2}, \quad \psi(\omega_1, \omega_2) = \frac{t''}{2t'}. \tag{4}$$

Bestimmt man ferner noch den Faktor C in (2) durch den speziellen Wert $u = 0$, so folgt

$$C = \frac{t'(\omega_1', \omega_2')}{t'(\omega_1, \omega_2)}. \tag{5}$$

Hiernach läßt sich die Formel (2) in folgendem Lehrsatz aussprechen:

Die Funktion

$$\sigma(u, \omega_1, \omega_2) = e^{-u^2\left(\frac{t'''}{6t'} - \frac{t''^2}{8t'^2}\right) - u\,\frac{t''}{2t'}}\,\frac{t(u, \omega_1, \omega_2)}{t'} \tag{6}$$

bleibt ungeändert, wenn man ω_1, ω_2 durch ω_1', ω_2' ersetzt d. h. wenn man irgend eine lineare Transformation anwendet, oder:

$$\sigma(u, \omega_1', \omega_2') = \sigma(u, \omega_1, \omega_2). \tag{7}$$

Die durch (6) definierte Funktion bleibt, wie eine einfache Rechnung zeigt, ungeändert, wenn man t durch irgend eine verwandte t-Funktion ersetzt.

Die Funktion $t(u)$ hat nach Voraussetzung die Charakteristik (1,1) und ihre Nullpunkte sind also kongruent mit 0. Demnach hat $t(-u)$ dieselben Nullpunkte und daher auch denselben Charakter wie $t(u)$. Beide Funktionen unterscheiden sich also nur durch einen Exponentialfaktor voneinander, und es ergibt sich leicht, wenn man einen konstanten Faktor aus $u = 0$ bestimmt:

$$t(-u) = -e^{2\pi i \mu u} t(u),$$

worin μ eine Konstante ist.

Differentiiert man diese Gleichung zweimal nach u und setzt dann $u = 0$, so folgt

$$2\pi i \mu = -\frac{t''}{t'},$$

und daraus ergibt sich nach (6), daß die Funktion $\sigma(u)$ der Bedingung

$$\sigma(-u) = -\sigma(u) \tag{8}$$

genügt, also eine **ungerade** Funktion von u ist.

Da $\sigma(u)$ eine t-Funktion erster Ordnung ist, so genügt es den beiden Bedingungen:

$$\sigma(u + \omega_1) = c_1 e^{\eta_1(2u + \omega_1)} \sigma(u),$$
$$\sigma(u + \omega_2) = c_2 e^{\eta_2(2u + \omega_2)} \sigma(u),$$

worin c_1, c_2, η_1, η_2 Konstanten sind. Die Funktion $\sigma(u)$ verschwindet für $u = 0$, aber nicht für $u = \frac{1}{2}\omega_1$, $u = \frac{1}{2}\omega_2$, und wenn man also in den vorstehenden Formeln $u = -\frac{1}{2}\omega_1$, $-\frac{1}{2}\omega_2$ setzt, so ergibt sich nach (8) $c_1 = -1$, $c_2 = -1$, also die Formeln:

$$\sigma(u + \omega_1) = -e^{\eta_1(2u + \omega_1)} \sigma(u), \tag{9}$$
$$\sigma(u + \omega_2) = -e^{\eta_2(2u + \omega_2)} \sigma(u).$$

Die hierdurch eingeführten η_1, η_2 sind Funktionen von ω_1, ω_2, die nach der Relation § 17, (10) (worin $\pi i a_1$, $\pi i a_2$, m durch $-\eta_1, -\eta_2$, 1 zu ersetzen ist) die Gleichung befriedigen:

$$\eta_1 \omega_2 - \eta_2 \omega_1 = \pi i. \tag{10}$$

Durch wiederholte Anwendung von (9) ergibt sich, wenn a, b ganze Zahlen sind [vgl. § 17, (16)]:

$$\sigma(u + a\omega_1 + b\omega_2) = (-1)^{a+b+ab} e^{(a\eta_1 + b\eta_2)(2u + a\omega_1 + b\omega_2)} \sigma(u). \tag{11}$$

Wenn man die Funktion $\sigma(u)$, wie sie durch die Formel (6) gegeben ist, nach Potenzen von u entwickelt, so findet sich, daß nicht nur die zweite, sondern auch die dritte Potenz von u in der Entwickelung nicht vorkommt, und man hat also:

$$\sigma(0) = 0, \quad \sigma'(0) = 1, \quad \sigma''(0) = 0, \quad \sigma'''(0) = 0. \tag{12}$$

Wenn auf ω_1, ω_2 eine lineare Substitution

$$(\omega_1', \omega_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (\omega_1, \omega_2) \tag{13}$$

angewendet wird, so erfahren die Größen η_1, η_2 die entsprechende Substitution

$$(\eta_1', \eta_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (\eta_1, \eta_2), \tag{14}$$

wie man unmittelbar aus den Relationen (7) und (11) folgert.

Differentiiert man die Formeln (9) logarithmisch nach u, so folgt

$$\begin{aligned} \frac{\sigma'(u + \omega_1)}{\sigma(u + \omega_1)} &= \frac{\sigma'(u)}{\sigma(u)} + 2\eta_1, \\ \frac{\sigma'(u + \omega_2)}{\sigma(u + \omega_2)} &= \frac{\sigma'(u)}{\sigma(u)} + 2\eta_2, \end{aligned} \tag{15}$$

und indem man in der ersten $u = -\frac{\omega_1}{2}$, in der zweiten $u = -\frac{\omega_2}{2}$ setzt, und beachtet, daß $\sigma(u)$ eine ungerade und folglich $\sigma'(u)$ eine gerade Funktion von u ist:

$$\eta_1 = \frac{\sigma'\left(\frac{\omega_1}{2}\right)}{\sigma\left(\frac{\omega_1}{2}\right)}, \quad \eta_2 = \frac{\sigma'\left(\frac{\omega_2}{2}\right)}{\sigma\left(\frac{\omega_2}{2}\right)}. \tag{16}$$

§ 36. Die Funktionen $\sigma_{00}, \sigma_{01}, \sigma_{10}$.

Es bleibt uns noch übrig, die analogen Resultate für die übrigen Charakteristiken zu gewinnen. Wir gehen aus von der folgenden Bemerkung: Sind x_1, x_2; y_1, y_2 irgend zwei Paare von Größen, welche durch dieselbe lineare Substitution S in x_1', x_2'; y_1', y_2' transformiert werden, ist also:

$$(x_1', x_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (x_1, x_2); \quad (y_1', y_2') = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} (y_1, y_2),$$

so ist auch

$$x_1 y_2 - x_2 y_1 = x_1' y_2' - x_2' y_1',$$

wie aus der Multiplikation der Determinanten hervorgeht. Demnach ist, was auch x_1, x_2 sei, nach (7), § 35:

$$(1) \quad \sigma(u + x_2 \omega_1 - x_1 \omega_2, \omega_1, \omega_2) = \sigma(u + x_2' \omega_1' - x_1' \omega_2', \omega_1', \omega_2').$$

Diese Funktion ändert sich der Formel (11) des vorigen Paragraphen gemäß, wenn x_1, x_2 um ganze Zahlen geändert werden. Diese Änderung kann man aber vermeiden, wenn man statt dessen die Funktion

$$e^{-2(\eta_1 x_2 - \eta_2 x_1) u} \frac{\sigma(u + x_2 \omega_1 - x_1 \omega_2)}{\sigma(x_2 \omega_1 - x_1 \omega_2)}$$

betrachtet, die wir (für den Augenblick) mit $\sigma(u, x_1, x_2, \omega_1, \omega_2)$ bezeichnen wollen. Diese Funktion genügt den Bedingungen:

$$(2) \quad \sigma(u, x_1', x_2', \omega_1', \omega_2') = \sigma(u, x_1, x_2, \omega_1, \omega_2),$$

$$(3) \quad \begin{aligned} \sigma(u, x_1 + 1, x_2, \omega_1, \omega_2) &= \sigma(u, x_1, x_2, \omega_1, \omega_2), \\ \sigma(u, x_1, x_2 + 1, \omega_1, \omega_2) &= \sigma(u, x_1, x_2, \omega_1, \omega_2), \end{aligned}$$

$$(4) \quad \begin{aligned} \sigma(u + \omega_1) &= -e^{-2\pi i x_1} e^{\eta_1 (2u + \omega_1)} \sigma(u), \\ \sigma(u + \omega_2) &= -e^{-2\pi i x_2} e^{\eta_2 (2u + \omega_2)} \sigma(u), \end{aligned}$$

und bleibt also ungeändert, wenn x_1 und x_2 um ganze Zahlen geändert werden.

Indem wir uns nun wieder auf die Hauptcharakteristiken beschränken, setzen wir $(x_1, x_2) = \left(-\frac{1}{2}, \frac{1}{2}\right), \left(0, \frac{1}{2}\right), \left(-\frac{1}{2}, 0\right)$ und erhalten so die folgenden drei Funktionen:

$$\sigma_{00}(u) = \sigma\left(u, -\frac{1}{2}, \frac{1}{2}, \omega_1, \omega_2\right) = e^{-(\eta_1 + \eta_2) u} \frac{\sigma\left(u + \frac{\omega_1 + \omega_2}{2}\right)}{\sigma\left(\frac{\omega_1 + \omega_2}{2}\right)},$$

$$(5) \quad \sigma_{10}(u) = \sigma\left(u, 0, \frac{1}{2}, \omega_1, \omega_2\right) = e^{-\eta_1 u} \frac{\sigma\left(u + \frac{\omega_1}{2}\right)}{\sigma\left(\frac{\omega_1}{2}\right)},$$

$$\sigma_{01}(u) = \sigma\left(u, -\frac{1}{2}, 0, \omega_1, \omega_2\right) = e^{-\eta_2 u} \frac{\sigma\left(u + \frac{\omega_2}{2}\right)}{\sigma\left(\frac{\omega_2}{2}\right)},$$

und die Funktion $\sigma(u)$ selbst kann entsprechend auch mit $\sigma_{11}(u)$ bezeichnet werden.

Für diese Funktionen ergeben sich nach (4) die charakteristischen Periodengleichungen

$$\begin{aligned} \sigma_{g_1,g_2}(u+\omega_1) &= (-1)^{g_1} e^{\eta_1(2u+\omega_1)} \sigma_{g_1,g_2}(u), \\ \sigma_{g_1,g_2}(u+\omega_2) &= (-1)^{g_2} e^{\eta_2(2u+\omega_2)} \sigma_{g_1,g_2}(u), \\ &\sigma_{g_1,g_2}(u+a\omega_1+b\omega_2) \\ &= (-1)^{g_1 a + g_2 b + ab} e^{(a\eta_1+b\eta_2)(2u+a\omega_1+b\omega_2)} \sigma_{g_1,g_2}(u). \end{aligned} \tag{6}$$

Durch Anwendung einer linearen Transformation werden die drei Funktionen σ_{00}, σ_{01}, σ_{10} untereinander permutiert, wie die Formel (2) lehrt [oder § 35, (1)]. Je nach dieser Permutation zerfallen die linearen Transformationen in sechs Klassen, deren erste alle die Transformationen umfaßt, die die Funktionen σ_{00}, σ_{01}, σ_{10} ungeändert lassen. Diese sind dadurch charakterisiert, daß α, δ ungerade, β, γ gerade Zahlen sind, was wir kurz so schreiben:

$$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} \pmod 2.$$

Hiernach sind die sechs Klassen der linearen Transformationen folgendermaßen zu charakterisieren:

$$\begin{array}{llcll} \text{I.} & \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv & \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} & \pmod 2 & (00, 01, 10), \\ \text{II.} & \quad " \quad \equiv & \begin{pmatrix}0, 1\\ -1, 0\end{pmatrix} & \quad " & (00, 10, 01), \\ \text{III.} & \quad " \quad \equiv & \begin{pmatrix}1, 1\\ -1, 0\end{pmatrix} & \quad " & (10, 00, 01), \\ \text{IV.} & \quad " \quad \equiv & \begin{pmatrix}1, 1\\ 0, 1\end{pmatrix} & \quad " & (10, 01, 00), \\ \text{V.} & \quad " \quad \equiv & \begin{pmatrix}1, 0\\ 1, 1\end{pmatrix} & \quad " & (01, 00, 10), \\ \text{VI.} & \quad " \quad \equiv & \begin{pmatrix}0, 1\\ -1, 1\end{pmatrix} & \quad " & (01, 10, 00), \end{array} \tag{7}$$

wo in der letzten Kolumne die jedesmalige Permutation der Charakteristiken 00, 01, 10 aufgeführt ist.

Die Transformationen der ersten Klasse bilden eine in der Gruppe aller linearen Substitutionen enthaltene Gruppe $\mathfrak{A}$, also einen Teiler der Gruppe $\mathfrak{L}$ (§ 28). Setzen wir

$$\alpha_1 = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}, \quad \alpha_2 = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} 1, & 1 \\ -1, & 0 \end{pmatrix},$$

$$\alpha_4 = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \quad \alpha_5 = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \quad \alpha_6 = \begin{pmatrix} 0, & 1 \\ -1, & 1 \end{pmatrix},$$

so sind $\alpha_1 \mathfrak{A}$, $\alpha_2 \mathfrak{A}$, $\alpha_3 \mathfrak{A}$, $\alpha_4 \mathfrak{A}$, $\alpha_5 \mathfrak{A}$, $\alpha_6 \mathfrak{A}$ die Nebengruppen zu $\mathfrak{A}$ und es ist

$$\mathfrak{L} = \alpha_1 \mathfrak{A} + \alpha_2 \mathfrak{A} + \alpha_3 \mathfrak{A} + \alpha_4 \mathfrak{A} + \alpha_5 \mathfrak{A} + \alpha_6 \mathfrak{A}$$

und $\mathfrak{A}$ ist ein Teiler von $\mathfrak{L}$ vom endlichen Index 6:

$$(\mathfrak{L}, \mathfrak{A}) = 6 \text{ (Bd. II, § 2).}$$

Die Gesamtheit $\alpha_1 \mathfrak{A} + \alpha_2 \mathfrak{A}$ ist ebenfalls eine Gruppe $\mathfrak{A}'$, und es ist

$$\mathfrak{L} = \alpha_1 \mathfrak{A}' + \alpha_3 \mathfrak{A}' + \alpha_4 \mathfrak{A}'$$

und $(\mathfrak{L}, \mathfrak{A}') = 3$.

So wie sämtliche lineare Transformationen aus den beiden Fundamentaltransformationen, so lassen sich die Transformationen der ersten Klasse aus wiederholter Anwendung von

$$\begin{pmatrix} 1, & 0 \\ 2, & 1 \end{pmatrix}, \quad \begin{pmatrix} 1, & 2 \\ 0, & 1 \end{pmatrix}, \quad \begin{pmatrix} -1, & 0 \\ 0, & -1 \end{pmatrix}$$

ableiten, was sich auf dem Wege des § 30 beweisen läßt.

§ 37. Darstellung der σ-Funktionen durch ϑ-Funktionen.

Um die Funktion $\sigma(u)$ als ϑ-Funktion darzustellen, kann man einfach die Formel (6) des § 35 auf die Funktion

$$t(u) = \vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)$$

anwenden, also

$$(1) \qquad \sigma(u, \omega_1, \omega_2) = \omega_1 e^{-\frac{u^2}{6\omega_1^2}\frac{\vartheta_{11}'''}{\vartheta_{11}'}} \frac{\vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{11}'}$$

setzen. Es ist aber infolge der Differentialgleichung § 20, (4):

$$\vartheta_{11}''' = 4\pi i \frac{d\vartheta_{11}'}{d\omega}$$

und also nach der Definition der Funktion $\eta(\omega)$ in § 34, (2):

$$(2) \qquad \frac{\vartheta_{11}'''}{\vartheta_{11}'} = 4\pi i \frac{d\log\vartheta_{11}'}{d\omega} = 12\pi i \frac{d\log\eta(\omega)}{d\omega}.$$

Durch logarithmische Differentiation von (1) erhält man mittels (2):

$$\frac{d \log \sigma(u)}{du} = -\frac{4\pi i u}{\omega_1^2} \frac{d \log \eta(\omega)}{d\omega} + \frac{d \log \vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{du},$$

und wenn man hierin $u = \frac{\omega_1}{2}, \frac{\omega_2}{2}$ setzt und die Formeln (8) des § 21 anwendet nach § 35, (16):

$$(3) \qquad \begin{aligned} \eta_1 &= -\frac{2\pi i}{\omega_1} \frac{d \log \eta(\omega)}{d\omega}, \\ \eta_2 &= -\frac{2\pi i \omega_2}{\omega_1^2} \frac{d \log \eta(\omega)}{d\omega} - \frac{\pi i}{\omega_1}. \end{aligned}$$

Hiernach kann man für σ setzen:

$$(4) \qquad \sigma(u) = \omega_1 e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta'_{11}},$$

und für die drei Funktionen $\sigma_{00}, \sigma_{01}, \sigma_{10}$ erhält man nach § 36, (5), wenn man einen konstanten Faktor aus

$$(5) \qquad \sigma_{00}(0) = 1, \quad \sigma_{01}(0) = 1, \quad \sigma_{10}(0) = 1$$

bestimmt:

$$(6) \qquad \begin{aligned} \sigma_{00}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{00}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{00}}, \\ \sigma_{01}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{01}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{01}}, \\ \sigma_{10}(u) &= e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{10}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{10}}. \end{aligned}$$

Die Funktionen $\sigma_{00}(u)$, $\sigma_{01}(u)$, $\sigma_{10}(u)$ sind gerade Funktionen von u, und durch zweimalige Differentiation der Logarithmen von (6) ergibt sich noch [nach (3) und § 34, (2)]:

$$(7) \qquad \sigma''_{00}(0) + \sigma''_{01}(0) + \sigma''_{10}(0) = 0.$$

Die Ausdrücke (4), (6) lassen auf den ersten Blick eine wichtige Eigenschaft der σ-Funktionen erkennen, daß nämlich $\sigma_{00}, \sigma_{01}, \sigma_{10}$ nur von den Verhältnissen $u : \omega_1 : \omega_2$ abhängen, während bei σ dasselbe, abgesehen von dem Faktor ω_1, gilt. Es sind also $\sigma, \sigma_{00}, \sigma_{01}, \sigma_{10}$ homogene Funktionen der drei

Variablen u, ω_1, ω_2 erstere von der ersten, die drei anderen von der nullten Ordnung, oder, in Zeichen, wenn λ einen willkürlichen Faktor bedeutet:

$$(8)\qquad \begin{aligned} \sigma(\lambda u\,,\,\lambda\omega_1,\lambda\omega_2) &= \lambda\sigma(u,\omega_1,\omega_2),\\ \sigma_{00}(\lambda u\,,\,\lambda\omega_1,\lambda\omega_2) &= \sigma_{00}(u,\omega_1,\omega_2),\\ \sigma_{01}(\lambda u\,,\,\lambda\omega_1,\lambda\omega_2) &= \sigma_{01}(u,\omega_1,\omega_2),\\ \sigma_{10}(\lambda u\,,\,\lambda\omega_1,\lambda\omega_2) &= \sigma_{10}(u,\omega_1,\omega_2). \end{aligned}$$

§ 38. Lineare Transformationen der Funktion $\eta(\omega)$.

Die Formeln (3), § 37 führen zur linearen Transformation der Funktion $\eta(\omega)$. Wird nämlich

$$(1)\qquad (\omega_1', \omega_2') = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(\omega_1, \omega_2)$$

gesetzt, so geht (η_1, η_2) über in

$$(2)\qquad (\eta_1', \eta_2') = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(\eta_1, \eta_2)$$

[§ 35, (14)] und $\omega = \omega_2 : \omega_1$ in

$$(3)\qquad \omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}.$$

Nun folgt aus (2) mit Rücksicht auf (3) des vorigen Paragraphen:

$$\eta_1' = -\frac{2\pi i}{\omega_1'}\frac{d\log\eta(\omega')}{d\omega'} = -\frac{2\pi i\omega_1'}{\omega_1^2}\frac{d\log\eta(\omega)}{d\omega} - \frac{\pi i\beta}{\omega_1},$$

$$\eta_2' = -\frac{2\pi i\omega_2'}{\omega_1'^2}\frac{d\log\eta(\omega')}{d\omega'} - \frac{\pi i}{\omega_1'} = -\frac{2\pi i\omega_2'}{\omega_1^2}\frac{d\log\eta(\omega)}{d\omega} - \frac{\pi i\delta}{\omega_1},$$

und diese beiden Relationen geben übereinstimmend

$$\frac{d\log\eta(\omega')}{\omega_1'^2\,d\omega'} = \frac{d\log\eta(\omega)}{\omega_1^2\,d\omega} + \frac{\beta}{2\,\omega_1\omega_1'},$$

oder endlich, da nach (3)

$$d\omega' = \frac{d\omega}{(\alpha+\beta\omega)^2},\quad \omega_1'^2\,d\omega' = \omega_1^2\,d\omega,$$

$$\frac{d\log\eta(\omega')}{d\omega} = \frac{d\log\eta(\omega)}{d\omega} + \frac{\beta}{2(\alpha+\beta\omega)}.$$

Hieraus folgt durch Integration:

$$(4)\qquad \eta\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = \varepsilon\sqrt{\alpha+\beta\omega}\;\eta(\omega),$$

worin ε eine von ω unabhängige, also nur von den Zahlen α, β, γ, δ abhängige Größe ist.

Die genaue Bestimmung dieser Konstanten ε, namentlich auch mit Rücksicht auf das Vorzeichen ist ein bekanntes wichtiges Problem, das eigentümliche Schwierigkeiten bietet, dessen Lösung aber für uns unerläßlich ist. Lösungen haben auf verschiedenen Wegen Hermite[1]) und Dedekind[2]), neuerdings auch Mertens und Scheibner[3]) gegeben. Wir wollen hier einen Weg gehen, der den Vorzug großer Einfachheit hat, dafür freilich nicht eine Ableitung, sondern nur einen Beweis der fertigen Formel enthält.

Für zwei spezielle Fälle haben wir schon früher [§ 34, (4), (5)] diese Bestimmung ausgeführt und auf dies Ergebnis werden wir uns hier stützen. Es sind die Formeln:

$$\eta(\omega \pm 1) = e^{\pm \frac{\pi i}{12}} \eta(\omega) \tag{5}$$

und

$$\eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\,\eta(\omega), \tag{6}$$

worin $\sqrt{-i\omega}$ mit positivem reellem Teil zu nehmen ist.

Wir setzen nun

$$\frac{\eta\left(\dfrac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)}{\eta(\omega)} = E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega\Big), \tag{7}$$

und haben den Wert dieses Symbols zu bestimmen. Nach (5), (6), (7) haben wir:

$$E\left(\begin{matrix}-\alpha, -\beta \\ -\gamma, -\delta\end{matrix}, \omega\right) = E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \omega\right), \tag{8}$$

$$E\left(\begin{matrix}1, 0 \\ 0, 1\end{matrix}, \omega\right) = 1, \tag{9}$$

$$E\left(\begin{matrix}1, 0 \\ \pm 1, 1\end{matrix}, \omega\right) = e^{\pm \frac{\pi i}{12}}, \tag{10}$$

$$E\left(\begin{matrix}0, 1 \\ -1, 0\end{matrix}, \omega\right) = \sqrt{-i\omega}. \tag{11}$$

---

[1]) Liouvilles Journal, Ser. II, T. III, 1858. Oeuvres de Charles Hermite, p. 487.

[2]) Erläuterungen zu Nr. XXVIII von Riemanns Werken, zweite Auflage und „Über die elliptischen Modulfunktionen", Crelles Journal, Bd. 83, S. 265. Vgl. auch des Verfassers Abhandlung „Zur Theorie der elliptischen Funktionen", Acta Mathematica, Bd. 6, S. 341 ff.

[3]) Mertens, Zur linearen Transformation der ϑ-Reihen, Transactions of the American mathematical society. July 1901. — Scheibner, Zur linearen Transformation der Theta-Funktionen und elliptischen Modulfunktionen, Berichte der Sächs. Gesellschaft der Wissenschaften. Oktober 1906.

Wir betrachten jetzt zwei Substitutionen und die aus beiden zusammengesetzte, also:

$$\begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix} = \begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}.$$

Ist dann

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

so ergibt sich aus der Definition (7):

$$(12) \qquad E\begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix}, \omega\Big) = E\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}, \omega'\Big) E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega\Big),$$

und davon zwei besondere Fälle, indem man

$$\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} = \begin{pmatrix}1, 0 \\ \pm 1, 1\end{pmatrix}, \quad \begin{pmatrix}0, 1 \\ -1, 0\end{pmatrix}$$

setzt und an Stelle von $\alpha', \beta', \gamma', \delta'$ wieder $\alpha, \beta, \gamma, \delta$ schreibt, also

$$\begin{pmatrix}\alpha'', \beta'' \\ \gamma'', \delta''\end{pmatrix} = \begin{pmatrix}\alpha \pm \beta, \beta \\ \gamma \pm \delta, \delta\end{pmatrix}, \quad \begin{pmatrix}-\beta, \alpha \\ -\delta, \gamma\end{pmatrix}:$$

$$(13) \qquad E\left(\begin{matrix}\alpha \pm \beta, \beta \\ \gamma \pm \delta, \delta\end{matrix}, \omega\right) = e^{\pm\frac{\pi i}{12}} E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \omega \pm 1\right),$$

$$(14) \qquad E\left(\begin{matrix}-\beta, \alpha \\ -\delta, \gamma\end{matrix}, \omega\right) = \sqrt{-i\omega}\, E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \frac{-1}{\omega}\right).$$

Es hat sich nun in § 30 gezeigt, daß sich alle linearen Transformationen durch wiederholte Anwendung der beiden Fundamentaltransformationen

$$\begin{pmatrix}1, 0 \\ 1, 1\end{pmatrix}, \quad \begin{pmatrix}0, 1 \\ -1, 0\end{pmatrix}$$

und ihrer inversen Transformationen zusammensetzen lassen, und daraus folgt auf Grund von (12), daß durch die Formeln (8) bis (14) das Symbol E vollständig definiert ist.

Wenn wir also einen diesen Bedingungen genügenden Ausdruck kennen, so muß dieser mit E übereinstimmen. Um einen solchen aufzustellen, unterscheiden wir zwei Fälle. Da α, β relative Primzahlen sind, so ist eine von ihnen sicher ungerade. Wir setzen:

(15)

1. α ungerade und positiv:

$$E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \omega\right) = \left(\frac{\beta}{\alpha}\right) i^{\frac{\alpha-1}{2}} e^{\frac{\pi i}{12}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]} \sqrt{(\alpha + \beta\omega)};$$

2. β ungerade und positiv:

$$E\left(\begin{matrix}\alpha, \beta \\ \gamma, \delta\end{matrix}, \omega\right) = \left(\frac{\alpha}{\beta}\right) i^{\frac{1-\beta}{2}} e^{\frac{\pi i}{12}[\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma]} \sqrt{-i(\alpha + \beta\omega)},$$

wozu noch folgendes zu bemerken ist: Die Wurzeln $\sqrt{\alpha+\beta\omega}$, $\sqrt{-i(\alpha+\beta\omega)}$ sind mit positivem reellem Teil zu nehmen. Daß eine von ihnen rein imaginär sei, ist durch die Annahme, daß ω einen positiven imaginären Teil hat und α bzw. β positiv sei, ausgeschlossen, denn danach kann $\alpha+\beta\omega$ oder $-i(\alpha+\beta\omega)$ nicht reell und negativ sein; $\left(\frac{\beta}{\alpha}\right)$ und $\left(\frac{\alpha}{\beta}\right)$ ist das Legendre-Jacobische Symbol aus der Theorie der quadratischen Reste, mit der Erweiterung, daß $\left(\frac{\beta}{1}\right)$ und $\left(\frac{0}{1}\right) = 1$ sein soll. Wenn im ersten Falle α oder im zweiten β negativ ist, so müssen rechts die sämtlichen Vorzeichen von α, β, γ, δ umgekehrt werden. Wenn sowohl α als β ungerade sind, so kann sowohl (15), 1. als (15), 2. angewandt werden, und beides ergibt, wie man leicht auf Grund des Reziprozitätsgesetzes der quadratischen Reste nachweist, dasselbe Resultat. Es ist nämlich, wenn α und β ungerade sind, α positiv angenommen wird, und das obere oder untere Zeichen gilt, je nachdem β positiv oder negativ ist:

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\pm\alpha}{\pm\beta}\right) = \pm e^{-\frac{\pi i}{4}(\alpha\mp 1)(\beta-1)},$$

$$\sqrt{\mp i(\alpha+\beta\omega)} = e^{\mp\frac{\pi i}{4}}\sqrt{\alpha+\beta\omega}$$

und die Identität von (15), 1., 2. ergibt sich dann aus den Kongruenzen

$$-3\alpha\beta+\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma \equiv \alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta \pmod{24},$$
$$\alpha\gamma+\alpha\beta \equiv \beta\delta \pmod{8},$$

von denen die zweite, wenn α und β beide nicht durch 3 teilbar, also $\alpha^2 \equiv \beta^2 \equiv 1 \pmod{3}$ sind, auch für den Modul 24 besteht.

Daß durch (15) die Formeln (8) bis (11) befriedigt sind, ist unmittelbar einzusehen, und es bleibt noch zu zeigen, daß (13) und (14) erfüllt sind. Wir beginnen mit (14), wobei angenommen werden kann, daß α ungerade (und positiv) sei; denn vertauscht man in (14) ω mit $-1:\omega$, so vertauschen sich α und $-\beta$, und diese können nicht beide gerade sein.

Es ist

$$\sqrt{-i\omega}\sqrt{\alpha-\frac{\beta}{\omega}} = \sqrt{-i(-\beta+\alpha\omega)};$$

denn setzen wir für den Augenblick

$$-i\omega = r e^{i\varphi}, \qquad \alpha - \frac{\beta}{\omega} = \varrho e^{i\psi}$$

$$-i(-\beta + \alpha\omega) = r\varrho e^{i(\varphi+\psi)},$$

so ist, da die reellen Teile von $-i\omega$, $-i(-\beta+\alpha\omega)$ positiv sin

$$-\frac{\pi}{2} < \varphi < \frac{\pi}{2}, \quad -\pi < \psi < \pi, \quad -\frac{\pi}{2} < \varphi + \psi < \frac{\pi}{2},$$

$$\sqrt{-i\omega} = \sqrt{r}\, e^{\frac{i\varphi}{2}}, \qquad \sqrt{\alpha - \frac{\beta}{\omega}} = \sqrt{\varrho}\, e^{\frac{i\psi}{2}},$$

und der reelle Teil von

$$\sqrt{-i\omega}\sqrt{\alpha - \frac{\beta}{\omega}} = \sqrt{-i(-\beta+\alpha\omega)} = \sqrt{r\varrho}\, e^{\frac{i(\varphi+\psi)}{2}}$$

positiv. Demnach ergibt sich aus (15), 1:

$$\sqrt{-i\omega}\, E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \frac{-1}{\omega}\Big)$$

$$= \left(\frac{\beta}{\alpha}\right) i^{\frac{\alpha-1}{2}} e^{\frac{\pi i}{12}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]} \sqrt{-i(-\beta+\alpha\omega)}.$$

Dieselbe Formel aber erhält man, da $\left(\frac{-\beta}{\alpha}\right) = i^{(\alpha-1)}\left(\frac{\beta}{\alpha}\right)$ aus (15), 2. für

$$E\begin{pmatrix}-\beta, \alpha \\ -\delta, \gamma\end{pmatrix}, \omega\Big),$$

und damit ist (14) bewiesen.

Es bleibt noch die Formel (13). Es genügt, die oberen Zeichen allein zu berücksichtigen, also die Formel

$$E\begin{pmatrix}\alpha+\beta, \beta \\ \gamma+\delta, \delta\end{pmatrix}, \omega\Big) = e^{\frac{\pi i}{12}} E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega + 1\Big)$$

zu beweisen, da der andere Fall durch Vertauschung von α, γ, ω mit $\alpha+\beta, \gamma+\delta, \omega+1$ auf diesen zurückkommt. Ist zunächs β ungerade (und positiv), so ergibt sich (13) aus (15), 2. au Grund der Kongruenz

$$(\beta^2-1)(1-\beta\gamma-\alpha\delta-\beta\delta) \equiv -\beta(\beta^2-1)(2\gamma+\delta) \equiv 0 \pmod{24}$$

Ist β gerade, so ist α ungerade. Nehmen wir α positiv, so kann $\alpha+\beta$ positiv oder negativ sein. Gelten im ersten Falle die oberen, im zweiten die unteren Zeichen, so ergibt uns (15), 1:

$$e^{\frac{i\pi}{12}} E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega + 1\Big)$$

(16)

$$= \left(\frac{\beta}{\alpha}\right) i^{-\frac{1-\alpha}{2}} e^{\frac{\pi i}{12}[1+\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]} \sqrt{\alpha+\beta+\beta\omega},$$

$$(17)\quad E\begin{pmatrix}\alpha+\beta, \beta \\ \gamma+\delta, \delta\end{pmatrix}, \omega)$$
$$= \left(\frac{\pm\beta}{\pm(\alpha+\beta)}\right) i^{-\frac{1\mp(\alpha+\beta)}{2}} e^{\frac{\pi i}{12}\{(\alpha+\beta)(\gamma+\delta-\beta)-[(\alpha+\beta)^2-1]\beta\delta\}} \sqrt{\pm(\alpha+\beta+\beta\omega)}.$$

Nun ist, wenn die unteren Zeichen gelten, β negativ, und wenn also

$$-(\alpha+\beta+\beta\omega) = r e^{i\varphi}$$
$$i(\alpha+\beta+\beta\omega) = r e^{i\left(\varphi-\frac{\pi}{2}\right)}$$

gesetzt wird, so liegt $\frac{\varphi}{2}$ und $\frac{\varphi}{2}-\frac{\pi}{4}$ zwischen $-\frac{\pi}{2}$ und $+\frac{\pi}{2}$, und daraus folgt, daß wir zu setzen haben:

$$\sqrt{-(\alpha+\beta+\beta\omega)} = i\sqrt{\alpha+\beta+\beta\omega},$$

ferner nach dem Reziprozitätsgesetz der quadratischen Reste:

$$\left(\frac{\beta}{\alpha+\beta}\right) = (-1)^{\frac{\beta(\alpha+1)}{4}}\left(\frac{\beta}{\alpha}\right),$$
$$\left(\frac{-\beta}{-(\alpha+\beta)}\right) = (-1)^{\frac{\alpha-1}{2}}(-1)^{\frac{\beta(\alpha-1)}{4}}\left(\frac{\beta}{\alpha}\right)\text{[1]},$$

und daraus folgt die Übereinstimmung der beiden Ausdrücke (16), (17) und mithin die Richtigkeit der Formel (13) nach der Kongruenz

$$\beta(3\alpha-2\gamma+\beta-\delta+\beta^2\delta+2\alpha\beta\delta) \equiv 0 \pmod{24},$$

die sich, da β gerade vorausgesetzt ist, aus $\alpha\delta-\beta\gamma=1$ ergibt.

Somit sind also die Formeln (15) als richtig erwiesen.

---

[1]) Nach dem Reziprozitätsgesetz ist, wenn $\beta = \pm 2^\lambda\beta'$ gesetzt und β' ungerade und positiv angenommen wird, wenn $\alpha+\beta$ positiv ist

$$\left(\frac{\beta}{\alpha+\beta}\right) = \left(\frac{\pm 2^\lambda}{\alpha+\beta}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha+\beta-1)(\beta'-1)}{4}},$$
$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{\pm 2^\lambda}{\alpha}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha-1)(\beta'-1)}{4}}.$$

Ist $\lambda \gtrless 2$, so sind diese beiden Werte einander gleich, ist $\lambda = 1$, so unterscheiden sie sich durch den Faktor $(-1)^{\frac{\alpha+1}{2}}$, in Übereinstimmung mit der ersten der obigen Formeln. Die Richtigkeit der zweiten Formel ergibt sich, wenn $\alpha+\beta$ negativ ist, aus

$$\left(\frac{-\beta}{-(\alpha+\beta)}\right) = \left(\frac{2^\lambda}{-(\alpha+\beta)}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{(\alpha+\beta-1)(\beta'-1)}{4}},$$
$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{2^\lambda}{\alpha}\right)\left(\frac{\alpha}{\beta'}\right)(-1)^{\frac{\alpha-1}{2}}(-1)^{\frac{(\alpha-1)(\beta'-1)}{4}}.$$

Setzen wir

$$(18)\qquad E\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}, \omega\Big) = \varepsilon\sqrt{\alpha + \beta\omega},$$

so ist ε eine 24ste Einheitswurzel, deren Produkt mit $\sqrt{\alpha + \beta\omega}$ durch (15) vollständig bestimmt ist, und es ergibt sich die Transformation der η-Funktion

$$(19)\qquad \eta\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \varepsilon\sqrt{\alpha + \beta\omega}\ \eta(\omega).$$

Für ε^{12} findet man

$$(20)\qquad \varepsilon^{12} = (-1)^{\alpha\beta + \gamma\delta + \beta\gamma}.$$

§ 39. Lineare Transformation der ϑ-Funktionen.

Die Transformationsformeln der ϑ-Funktionen sind Folgen der Grundeigenschaften der σ-Funktion, durch die Substitution

$$(\omega_1', \omega_2') = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}(\omega_1, \omega_2)$$

ungeändert zu bleiben. Aus § 37, (4) ergibt sich hiernach, wenn man $\omega_1, \omega_2, \eta_1$ durch $\omega_1', \omega_2', \eta_1'$ ersetzt:

$$\frac{\omega_1 e^{\frac{\eta_1 u^2}{\omega_1}}\vartheta_{11}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{11}'\left(0, \frac{\omega_2}{\omega_1}\right)} = \frac{\omega_1' e^{\frac{\eta_1' u^2}{\omega_1'}}\vartheta_{11}\left(\frac{u}{\omega_1'}, \frac{\omega_2'}{\omega_1'}\right)}{\vartheta_{11}'\left(0, \frac{\omega_2'}{\omega_1'}\right)},$$

oder, weil nach § 35, (10), (13), (14)

$$(1)\qquad \frac{\eta_1}{\omega_1} - \frac{\eta_1'}{\omega_1'} = \frac{\omega_1'\eta_1 - \eta_1'\omega_1}{\omega_1\omega_1'} = \beta\,\frac{\omega_2\eta_1 - \omega_1\eta_2}{\omega_1\omega_1'} = \frac{\pi i\beta}{\omega_1\omega_1'}$$

ist, wenn wir:

$$(2)\qquad \begin{gathered} v = \frac{u}{\omega_1}, \qquad \omega = \frac{\omega_2}{\omega_1}, \\ v' = \frac{u}{\omega_1'} = \frac{v}{\alpha + \beta\omega}, \qquad \omega' = \frac{\omega_2'}{\omega_1'} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega} \end{gathered}$$

setzen:

$$\frac{\vartheta_{11}(v', \omega')}{\vartheta_{11}'(0, \omega')} = \frac{e^{\pi i\beta v v'}}{\alpha + \beta\omega}\,\frac{\vartheta_{11}(v, \omega)}{\vartheta_{11}'(0, \omega)}.$$

Es ist ferner

$$\vartheta_{11}'(0, \omega) = 2\pi\eta(\omega)^3, \qquad \vartheta_{11}'(0, \omega') = 2\pi\eta(\omega')^3,$$

woraus nach § 38, (19):

$$\vartheta_{11}'(0, \omega') = \varepsilon^3\sqrt{\alpha + \beta\omega}^{\,3}\,\vartheta_{11}'(0, \omega),$$

und daraus endlich:

(3) $$e^{-\pi i\beta v v'}\vartheta_{11}(v', \omega') = \varepsilon^3\sqrt{\alpha+\beta\omega}\,\vartheta_{11}(v, \omega).$$

Die Transformationsformeln der drei übrigen Funktionen $\vartheta_{00}, \vartheta_{01}, \vartheta_{10}$ sind verschieden in den sechs Klassen des § 36 und können aus den Formeln (5), § 36 in derselben Weise hergeleitet werden. Man kann die sechs Fälle aber auch in ein einziges Formelsystem zusammenfassen, das man aus (3) erhält, wenn man v ersetzt durch

$$v + \frac{\alpha+\beta\omega}{2}, \qquad v + \frac{\gamma+\delta\omega}{2}, \qquad v + \frac{\alpha+\gamma+(\beta+\delta)\omega}{2},$$

also v' durch

$$v' + \frac{1}{2}, \qquad v' + \frac{\omega'}{2}, \qquad v' = \frac{1+\omega'}{2},$$

und dann auf der rechten und linken Seite von (3) die Formeln (2), (3), (8) des § 21 anwendet. So kommt:

(4) $$e^{-\pi i\beta v v'}\vartheta_{10}(v', \omega') = i^\beta e^{-\frac{\pi i\alpha\beta}{4}}\varepsilon^3\sqrt{\alpha+\beta\omega}\,\vartheta_{1+\beta,\,1-\alpha}(v, \omega),$$

(5) $$e^{-\pi i\beta v v'}\vartheta_{01}(v', \omega') = i^{\delta-1} e^{-\frac{\pi i\gamma\delta}{4}}\varepsilon^3\sqrt{\alpha+\beta\omega}\,\vartheta_{1+\delta,\,1-\gamma}(v, \omega),$$

(6) $$e^{-\pi i\beta v v'}\vartheta_{00}(v', \omega') = i^{\delta+\beta-\alpha\delta} e^{-\frac{\pi i}{4}(\alpha\beta+\gamma\delta)}\varepsilon^3\sqrt{\alpha+\beta\omega}\,\vartheta_{1+\beta+\delta,\,1-\alpha-\gamma}(v, \omega).$$

Die vierten Potenzen dieser Funktionen lassen sich einfacher ausdrücken durch

(7) $$e^{-4\pi i\beta v v'}\vartheta^4_{g_1, g_2}(v', \omega') = (-1)^{g_2\alpha\beta+g_1\gamma\delta+\beta\gamma}(\alpha+\beta\omega)^2\vartheta^4_{g'_1, g'_2}(v),$$

worin in den sechs Klassen die zu den Charakteristiken $(g_1, g_2) = (00), (01), (10)$ gehörigen Charakteristiken (g'_1, g'_2) aus der letzten Kolumne der Tabelle in § 36 zu entnehmen sind.

Eine einfachere Transformationsformel erhält man aus den σ-Funktionen für das Produkt der drei ϑ-Funktionen (4), (5), (6). Es ist nämlich, wenn man das Produkt der drei Funktionen § 37, (6) bildet:

$$\sigma_{00}(u)\,\sigma_{01}(u)\,\sigma_{10}(u) = e^{\frac{3\eta_1 u^2}{\omega_1}}\frac{\vartheta_{00}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)\vartheta_{01}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)\vartheta_{10}\left(\frac{u}{\omega_1}, \frac{\omega_2}{\omega_1}\right)}{\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}}$$

eine Funktion, die nach § 36 bei linearer Transformation völlig ungeändert bleibt. Macht man noch Gebrauch von der Relation (2):

$$\eta_1' \omega_1 - \eta_1 \omega_1' = -\pi i \beta,$$

so folgt

$$\text{(8)} \qquad \begin{aligned} &\frac{\vartheta_{00}(v, \omega)\,\vartheta_{01}(v, \omega)\,\vartheta_{10}(v, \omega)}{\vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}} \\ &= e^{-3\pi i \beta v v'} \frac{\vartheta_{00}(v', \omega')\,\vartheta_{01}(v', \omega')\,\vartheta_{10}(v', \omega')}{\vartheta_{00}(0, \omega')\,\vartheta_{01}(0, \omega')\,\vartheta_{10}(0, \omega')}, \end{aligned}$$

worin man noch nach (19) des vorigen Paragraphen

$$\vartheta_{00}(0, \omega')\,\vartheta_{01}(0, \omega')\,\vartheta_{10}(0, \omega') = \varepsilon^3 \sqrt{\alpha + \beta\omega}^{\,3}\, \vartheta_{00}\,\vartheta_{01}\,\vartheta_{10}$$

setzen kann.

Wir ziehen aber aus (8) einen anderen Schluß: Setzt man nämlich

$$v' = \frac{h}{n}, \qquad v = \frac{h(\alpha + \beta\omega)}{n},$$

und nimmt das Produkt für $h = 1, 2, \cdots, \frac{n-1}{2}$, so ergibt sich mittels der bekannten Relation (Bd. I, § 11)

$$\sum_{1, \frac{n-1}{2}}^{h} h^2 = n \frac{n^2 - 1}{24},$$

wenn man auf der rechten Seite von (8) die Formel (23), § 32 anwendet:

$$\text{(9)} \qquad \begin{aligned} &2^{\frac{n-1}{2}} \prod_{1, \frac{n-1}{2}}^{h} \vartheta_{00}\left(\frac{h(\alpha + \beta\omega)}{n}\right) \vartheta_{01}\left(\frac{h(\alpha + \beta\omega)}{n}\right) \vartheta_{10}\left(\frac{h(\alpha + \beta\omega)}{n}\right) \\ &= e^{-\frac{\pi i}{8} \frac{n^2 - 1}{n} \beta(\alpha + \beta\omega)}\, \vartheta_{00}^{\frac{n-1}{2}}\, \vartheta_{01}^{\frac{n-1}{2}}\, \vartheta_{01}^{\frac{n-1}{2}}, \end{aligned}$$

worin nun α, β irgend ein Paar relativer Primzahlen sein kann.

§ 40. Lineare Transformation der Funktionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$.

Die Formeln für die lineare Transformation der f-Funktionen sind nach § 34, (9) eine einfache Folge der Transformation der η-Funktion.

Setzen wir in der linearen Transformation

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

zunächst β als gerade und folglich α, δ als ungerade voraus, so ist

$$(1) \qquad \begin{pmatrix}1, & 0\\0, & 2\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\\gamma, & \delta\end{pmatrix} = \begin{pmatrix}\alpha, & \frac{1}{2}\beta\\2\gamma, & \delta\end{pmatrix}\begin{pmatrix}1, & 0\\0, & 2\end{pmatrix},$$

d. h.

$$2\,\frac{\gamma+\delta\omega}{\alpha+\beta\omega} = \frac{2\gamma+\delta \, . \, 2\omega}{\alpha+\frac{1}{2}\beta \, . \, 2\omega}.$$

Es ist aber nach § 34, (9):

$$f_2(\omega) = \sqrt{2}\,\frac{\eta(2\omega)}{\eta(\omega)},$$

und wenn wir also die Substitution

$$\omega, \frac{\gamma+\delta\omega}{\alpha+\beta\omega}$$

machen, so ergibt sich, mit Benutzung der Bezeichnung des § 38

$$(2) \qquad f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = \frac{E\begin{pmatrix}\alpha, & \frac{1}{2}\beta\\2\gamma, & \delta\end{pmatrix}, 2\omega}{E\begin{pmatrix}\alpha, & \beta\\\gamma, & \delta\end{pmatrix}, \omega}\, f_2(\omega).$$

Hier sind die E-Funktionen nach § 38, (15), 1. zu bestimmen, woraus sich ergibt:

$$\frac{E\begin{pmatrix}\alpha, & \frac{1}{2}\beta\\2\gamma, & \delta\end{pmatrix}, 2\omega}{E\begin{pmatrix}\alpha, & \beta\\\gamma, & \delta\end{pmatrix}, \omega} = \left(\frac{2}{\alpha}\right) e^{\frac{\pi i}{12}\left(\alpha\gamma+\frac{\alpha\beta}{2}+(\alpha^2-1)\frac{\beta\delta}{2}\right)}.$$

Es ist aber $\frac{1}{24} = \frac{3}{8} - \frac{1}{3}$ und

$$\alpha\gamma + \frac{\alpha\beta}{2} + (\alpha^2-1)\frac{\beta\delta}{2} \equiv \frac{\alpha(2\gamma+\beta)}{2} \pmod 8$$
$$\equiv \alpha(\gamma-\beta) - (\alpha^2-1)\beta\delta \pmod 3,$$

und wenn wir also zur Abkürzung

$$(3) \qquad \varrho = e^{-\frac{2\pi i}{3}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]}$$

setzen, so ergibt sich aus (2):

$$(4) \qquad f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) = \left(\frac{2}{\alpha}\right)\varrho\, e^{\frac{3\pi i}{8}\alpha(2\gamma+\beta)} f_2(\omega), \qquad \beta \equiv 0 \pmod 2.$$

In derselben Weise lassen sich alle anderen Formeln dieser Art herleiten; man erhält sie aber einfacher aus (4) selbst mit Benutzung der Fundamentaltransformationen § 34, (13), (14), (15). So ergibt sich, wenn man in (4) ω durch $-1:\omega$ ersetzt und dann $\alpha, \beta, \gamma, \delta$ mit $\beta, -\alpha, \delta, -\gamma$ vertauscht (wodurch ϱ ungeändert bleibt):

$$(5)\quad f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=\left(\frac{2}{\beta}\right)\varrho\, e^{\frac{3\pi i}{8}\beta(2\delta-\alpha)} f_1(\omega),\qquad \alpha\equiv 0 \pmod 2,$$

und ersetzt man hierin ω durch $\omega+3$ und γ, α durch $\gamma-3\delta$, $\alpha-3\beta$, so folgt

$$(6)\quad f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=-\varrho\, e^{\frac{3\pi i}{8}\beta(2\delta-\alpha)} f(\omega),\quad \alpha-\beta\equiv 0 \pmod 2.$$

Setzt man in (4), (5), (6)

$$f_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=f_1\left(-\frac{\alpha+\beta\omega}{\gamma+\delta\omega}\right),$$

und vertauscht dann α, β, γ, δ mit $-\gamma$, $-\delta$, α, β, so ergibt sich

$$(7)\quad f_1\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=\left(\frac{2}{\gamma}\right)\varrho\, e^{-\frac{3\pi i}{8}\gamma(2\alpha-\delta)} f_2(\omega),\qquad \delta\equiv 0 \pmod 2,$$

$$(8)\quad =\left(\frac{2}{\delta}\right)\varrho\, e^{-\frac{3\pi i}{8}\delta(2\beta+\gamma)} f_1(\omega),\qquad \gamma\equiv 0 \pmod 2,$$

$$(9)\quad =-\varrho\, e^{-\frac{3\pi i}{8}\delta(2\beta+\gamma)} f(\omega),\ \gamma-\delta\equiv 0 \pmod 2.$$

Aus (9) und (6) erhält man, indem man ω durch $\frac{-\gamma+\alpha\omega}{\delta-\beta\omega}$ und dann α, β, γ, δ durch δ, $-\beta$, $-\gamma$, α ersetzt:

$$(10)\quad f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=-\varrho\, e^{-\frac{3\pi i}{8}\alpha(2\beta+\gamma)} f_1(\omega),\quad \alpha-\gamma\equiv 0 \pmod 2,$$

$$(11)\quad f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=-\varrho\, e^{\frac{3\pi i}{8}\beta(2\alpha-\delta)} f_2(\omega),\qquad \beta-\delta\equiv 0 \pmod 2,$$

und wenn man endlich in (10) ω durch $\omega+9$ und γ, α durch $\gamma-9\delta$, $\alpha-9\beta$ ersetzt:

$$(12)\quad f\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right)=\varrho\left(\frac{2}{\alpha-\beta}\right) e^{-\frac{3\pi i}{8}(\alpha-\beta)(\alpha+\beta+\gamma-\delta)} f(\omega),$$

$$\alpha+\beta+\gamma-\delta\equiv 0 \pmod 2)\ [1].$$

[1]) Die von Hermite (Sur la théorie des équations modulaires, Paris 1859) eingeführten Funktionen $\varphi(\omega)$, $\psi(\omega)$, $\chi(\omega)$ hängen mit den Funktionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ durch die Gleichungen

$$f(\omega)=\frac{\sqrt[6]{2}}{\chi(\omega)},\quad f_1(\omega)=\sqrt[6]{2}\,\frac{\psi(\omega)}{\chi(\omega)},\quad f_2(\omega)=\sqrt[6]{2}\,\frac{\varphi(\omega)}{\chi(\omega)}$$

zusammen. Die Transformationsformeln der f-Funktionen lassen sich mit Benutzung der Relation $\alpha\delta-\beta\gamma=1$ auf mannigfaltige Weise umgestalten. So sind die von Hermite a. a. O. angegebenen Formeln nicht ohne weiteres mit den unserigen als identisch zu erkennen. Eine einfache Rechnung zeigt aber ihre Übereinstimmung. Die oben gegebenen Formeln haben den Vorzug, daß sie, ohne an Einfachheit zu verlieren, je zwei der sechs Transformationsklassen in einen Ausdruck zusammenfassen.

Vierter Abschnitt.

Die elliptischen Funktionen.

§ 41. Zusammenhang der ϑ-Funktionen mit den elliptischen Integralen.

Nach § 21 bestehen zwischen den Quadraten der vier ϑ-Funktionen zwei voneinander unabhängige lineare Gleichungen, und man kann also zwei von diesen Quadraten durch die beiden anderen oder auch alle vier durch zwei unabhängige Variable ξ, η ausdrücken. Indem wir das letztere tun, bezeichnen wir mit ξ_1, η_1; ξ_2, η_2; ξ_3, η_3; ξ_4, η_4 Konstanten und setzen, indem wir an die Bezeichnungsweise Bd. I, § 67 anknüpfen:

$$(1)\qquad \begin{aligned} \vartheta_{01}^2(u) &= \xi\eta_1 - \eta\xi_1 = (\xi\eta_1), \\ \vartheta_{11}^2(u) &= \xi\eta_2 - \eta\xi_2 = (\xi\eta_2), \\ \vartheta_{10}^2(u) &= \xi\eta_3 - \eta\xi_3 = (\xi\eta_3), \\ \vartheta_{00}^2(u) &= \xi\eta_4 - \eta\xi_4 = (\xi\eta_4). \end{aligned}$$

Zwischen den Konstanten ξ_i, η_i und den Werten ϑ_{01}, ϑ_{10}, ϑ_{00} bestehen vier Relationen, die sich aus den Gleichungen (13) des § 21 herleiten lassen. Diese Gleichungen können wir nach der Bezeichnung (1) in der Form schreiben:

$$(2)\qquad \begin{aligned} (\xi\eta_3)\vartheta_{01}^2 &= (\xi\eta_1)\vartheta_{10}^2 - (\xi\eta_2)\vartheta_{00}^2, \\ (\xi\eta_4)\vartheta_{01}^2 &= (\xi\eta_1)\vartheta_{00}^2 - (\xi\eta_2)\vartheta_{10}^2. \end{aligned}$$

Man kann diesen Relationen, indem man in (2) $\xi, \eta = \xi_1, \eta_1$ und $= \xi_2, \eta_2$ setzt, die Form geben:

$$(3)\qquad \begin{aligned} (\xi_1\eta_3)\vartheta_{01}^2 &= (\xi_2\eta_1)\vartheta_{00}^2, \\ (\xi_2\eta_3)\vartheta_{01}^2 &= (\xi_2\eta_1)\vartheta_{10}^2, \\ (\xi_1\eta_4)\vartheta_{01}^2 &= (\xi_2\eta_1)\vartheta_{10}^2, \\ (\xi_2\eta_4)\vartheta_{01}^2 &= (\xi_2\eta_1)\vartheta_{00}^2, \end{aligned}$$

wozu man noch fügen kann, indem man in (2) $\xi, \eta = \xi_4, \eta_4$ setzt und (3) und § 21, (14) benutzt:

$$(4)\qquad (\xi_4\eta_3) = (\xi_2\eta_1).$$

Aus (3) und (4) folgt für die Doppelverhältnisse:

(5) $$\frac{(\xi_2\eta_3)(\xi_1\eta_4)}{(\xi_1\eta_3)(\xi_2\eta_4)} = \frac{\vartheta_{10}^4}{\vartheta_{00}^4},$$

(6) $$\frac{(\xi_1\eta_2)(\xi_3\eta_4)}{(\xi_1\eta_3)(\xi_2\eta_4)} = \frac{\vartheta_{01}^4}{\vartheta_{00}^4}.$$

Wenn wir nun zwei der Gleichungen (1), etwa die beiden ersten, differentiieren, so folgt:

$$2\,\vartheta_{01}(u)\,\vartheta_{01}'(u)\,du = \eta_1\,d\xi - \xi_1\,d\eta = (\eta_1\,d\xi),$$
$$2\,\vartheta_{11}(u)\,\vartheta_{11}'(u)\,du = \eta_2\,d\xi - \xi_2\,d\eta = (\eta_2\,d\xi),$$

und daraus mit Benutzung von (1)

$$\begin{aligned} 2\,\vartheta_{01}(u)\,\vartheta_{11}(u)\,[\vartheta_{01}'(u)\,\vartheta_{11}(u) - \vartheta_{11}'(u)\,\vartheta_{01}(u)]\,du \\ = (\eta_1\,d\xi)\,\vartheta_{11}^2(u) - (\eta_2\,d\xi)\,\vartheta_{01}^2(u) \\ = (\eta_1\,d\xi)(\xi\,\eta_2) - (\eta_2\,d\xi)(\xi\,\eta_1) = (\xi_2\,\eta_1)(\xi\,d\eta). \end{aligned}$$

Den letzten Ausdruck kann man ohne Rechnung dadurch ableiten, daß man den vorletzten als lineare Funktion von $d\xi$, $d\eta$ betrachtet, die für $d\xi : d\eta = \xi : \eta$ verschwindet und daher durch $(\xi\,d\eta)$ teilbar ist. Den Quotienten $(\xi_2\,\eta_1)$ erhält man, wenn man $d\xi : d\eta = \xi_2 : \eta_2$ setzt. Mit Benutzung von § 23, (6) erhält man dann

(7) $$2\pi\,\vartheta_{01}^2\,\vartheta_{00}(u)\,\vartheta_{11}(u)\,\vartheta_{10}(u)\,\vartheta_{01}(u)\,du = (\xi_1\,\eta_2)(\xi\,d\eta).$$

Führt man hierin nach (3) (erste und letzte Formel)

(8) $$(\xi_1\,\eta_2)\,\vartheta_{00}^2 = \sqrt{(\xi_1\,\eta_3)(\xi_2\,\eta_4)}\;\vartheta_{01}^2$$

ein, und setzt für die ϑ-Funktionen die Ausdrücke (1), so folgt schließlich

(9) $$2\pi\,\vartheta_{00}^2\,du = \frac{\sqrt{(\xi_1\,\eta_3)(\xi_2\,\eta_4)}\,(\xi\,d\eta)}{\sqrt{(\xi\,\eta_1)(\xi\,\eta_2)(\xi\,\eta_3)(\xi\,\eta_4)}},$$

wodurch du als elliptisches Differential erster Gattung in homogenen Variablen [§ 1, (5)] dargestellt ist.

Es ist durch (1) das Verhältnis $\xi : \eta$ als doppeltperiodische Funktion von u bestimmt. Desgleichen sind aber auch die Verhältnisse der Quadratwurzeln

(10) $$\sqrt{(\xi\,\eta_1)},\quad \sqrt{(\xi\,\eta_2)},\quad \sqrt{(\xi\,\eta_3)},\quad \sqrt{(\xi\,\eta_4)}$$

als eindeutige doppeltperiodische Funktionen erklärt, und das Vorzeichen der Quadratwurzeln in (9) ist hierdurch und durch (8) ebenfalls eindeutig bestimmt.

Ist ω der Modul der ϑ-Funktionen, so gehören, wie sich nach (1) aus dem Verschwinden der vier ϑ-Funktionen ergibt, die folgenden Werte zusammen:

$$(11) \qquad \begin{aligned} u &= \tfrac{1}{2}\omega, & \xi:\eta &= \xi_1:\eta_1, \\ u &= 0, & \xi:\eta &= \xi_2:\eta_2, \\ u &= \tfrac{1}{2}, & \xi:\eta &= \xi_3:\eta_3, \\ u &= \frac{1+\omega}{2}, & \xi:\eta &= \xi_4:\eta_4. \end{aligned}$$

§ 42. Jacobis elliptische Funktionen.

Da man die Variablen ξ, η mittels einer linearen Substitution, in der vier Koeffizienten disponibel sind, durch zwei neue Variable ersetzen kann, so kann man vier von der Größe ξ_i, η_i oder drei von ihren Verhältnissen beliebige Werte erteilen, ohne die Allgemeinheit zu beeinträchtigen.

Wir wollen setzen

$$(1) \qquad \xi_1 = 0, \qquad \eta_2 = 0, \qquad \xi_3 = \eta_3,$$

und führen noch $\varkappa^2$, $\varkappa'^2$, ζ durch die Gleichungen an:

$$(2) \qquad \xi_4 = \varkappa^2 \eta_4, \qquad \varkappa'^2 = 1 - \varkappa^2, \qquad \frac{\eta}{\xi} = \zeta.$$

Aus § 41, (3), (5), (6) ergibt sich dann

$$(3) \qquad \begin{gathered} \frac{\xi_2}{\eta_1} = -\frac{\vartheta_{10}^2}{\vartheta_{00}^2}, \qquad \frac{\eta_3}{\eta_1} = \frac{\vartheta_{10}^2}{\vartheta_{01}^2}, \qquad \frac{\eta_4}{\eta_1} = \frac{\vartheta_{00}^2}{\vartheta_{01}^2}, \\ \sqrt{\varkappa} = \frac{\vartheta_{10}}{\vartheta_{00}}, \qquad \sqrt{\varkappa'} = \frac{\vartheta_{01}}{\vartheta_{00}}, \end{gathered}$$

und aus (1), (9), § 41 findet sich:

$$(4) \qquad \begin{aligned} \frac{\vartheta_{00}}{\vartheta_{10}} \frac{\vartheta_{11}(u)}{\vartheta_{01}(u)} &= \sqrt{\zeta}, \\ \frac{\vartheta_{01}}{\vartheta_{10}} \frac{\vartheta_{10}(u)}{\vartheta_{01}(u)} &= \sqrt{1-\zeta}, \\ \frac{\vartheta_{01}}{\vartheta_{00}} \frac{\vartheta_{00}(u)}{\vartheta_{01}(u)} &= \sqrt{1-\varkappa^2\zeta}. \end{aligned}$$

$$(5) \qquad 2\pi \vartheta_{00}^2 u = \int_0^\zeta \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

worin der Integrationsweg und die Bedeutung der Wurzelzeichen durch die Formeln (4) selbst bestimmt ist, wenn der Übergang

von 0 zu u in der u-Ebene gegeben ist. Es darf aber dann auch der Integrationsweg in (5) geändert werden, wenn dabei nur keiner der singulären Punkte ∞, 1, $\frac{1}{\varkappa^2}$ überschritten wird.

Die Gleichung (5) läßt sich in folgenden drei Formen schreiben:

$$(6)\qquad \begin{aligned} d\sqrt{\xi} &= \pi\vartheta_{00}^2\sqrt{(1-\xi)(1-\varkappa^2\xi)}\,du, \\ d\sqrt{1-\xi} &= -\pi\vartheta_{00}^2\sqrt{\xi(1-\varkappa^2\xi)}\,du, \\ d\sqrt{1-\varkappa^2\xi} &= -\pi\vartheta_{00}^2\varkappa^2\sqrt{\xi(1-\xi)}\,du. \end{aligned}$$

Führen wir eine neue Variable v ein durch die Gleichung

$$(7)\qquad \pi\vartheta_{00}^2 u = v,$$

so werden die Gleichungen (5), (6):

$$(8)\qquad v = \frac{1}{2}\int_0^\xi \frac{d\xi}{\sqrt{\xi(1-\xi)(1-\varkappa^2\xi)}},$$

$$(9)\qquad \begin{aligned} d\sqrt{\xi} &= \sqrt{(1-\xi)(1-\varkappa^2\xi)}\,dv, \\ d\sqrt{1-\xi} &= -\sqrt{\xi(1-\varkappa^2\xi)}\,dv, \\ d\sqrt{1-\varkappa^2\xi} &= -\varkappa^2\sqrt{\xi(1-\xi)}\,dv, \end{aligned}$$

und nun betrachten wir die drei Größen $\sqrt{\xi} = x$, $\sqrt{1-\xi} = y$, $\sqrt{1-\varkappa^2\xi} = z$ durch (4) und (7) als Funktionen der Variablen v definiert. Nach (4) sind es eindeutige, doppeltperiodische und, abgesehen von einzelnen Punkten, in denen sie unendlich werden, stetige Funktionen von v. Sie werden nach Jacobi sinus amplitudinis, cosinus amplitudinis, Δ amplitudinis von v genannt und mit $\operatorname{sinam} v$, $\operatorname{cosam} v$, $\Delta \operatorname{am} v$ bezeichnet. Wir wollen uns hier der schon in § 14 erwähnten kürzeren Gudermannschen Bezeichnung $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ bedienen, wonach

$$(10)\qquad \begin{aligned} \frac{\vartheta_{11}(u)}{\vartheta_{01}(u)} &= \sqrt{\varkappa}\operatorname{sn} v, \\ \frac{\vartheta_{10}(u)}{\vartheta_{01}(u)} &= \sqrt{\frac{\varkappa}{\varkappa'}}\operatorname{cn} v, \\ \frac{\vartheta_{00}(u)}{\vartheta_{01}(u)} &= \frac{1}{\sqrt{\varkappa'}}\operatorname{dn} v. \end{aligned}$$

Diese Funktionen genügen nach (9) den Differentialgleichungen

$$\frac{dx}{dv} = yz,$$

(11) $$\frac{dy}{dv} = -zx,$$

$$\frac{dz}{dv} = -\varkappa^2 xy,$$

und den Nebenbedingungen:

(12) $$\operatorname{sn} 0 = 0, \quad \operatorname{cn} 0 = 1, \quad \operatorname{dn} 0 = 1.$$

Es bestehen zwischen ihnen die Relationen

(13) $$y^2 = 1 - x^2, \quad z^2 = 1 - \varkappa^2 x^2.$$

Aus den Fundamentaleigenschaften der ϑ-Funktionen ergeben sich die ersten Eigenschaften der elliptischen Funktionen:

$$\operatorname{sn} v = -\operatorname{sn}(-v), \quad \operatorname{cn} v = \operatorname{cn}(-v), \quad \operatorname{dn} v = \operatorname{dn}(-v),$$

d. h. $\operatorname{sn} v$ ist eine ungerade, $\operatorname{cn} v$, $\operatorname{dn} v$ sind gerade Funktionen.

Setzen wir noch

(14) $$\pi \vartheta_{00}^2 = 2K, \quad \pi \vartheta_{00}^2 \omega = 2iK',$$

und folglich

(15) $$\pi \vartheta_{01}^2 = 2\varkappa' K, \quad \pi \vartheta_{10}^2 = 2\varkappa K, \quad \omega = \frac{iK'}{K},$$

so erhält v die Werte K, iK', $K + iK'$, wenn $u = \frac{1}{2}, \frac{\omega}{2}, \frac{1+\omega}{2}$ wird, und es folgt aus (4) mit Rücksicht auf (3) und § 21, (10):

$$\operatorname{sn} K = 1, \quad \operatorname{sn}(K + iK') = \frac{1}{\varkappa},$$

(16) $$\operatorname{cn} K = 0, \quad \operatorname{cn}(K + iK') = -\frac{i\varkappa'}{\varkappa},$$

$$\operatorname{dn} K = \varkappa', \quad \operatorname{dn}(K + iK') = 0,$$

$$\operatorname{sn} iK', \quad \operatorname{cn} iK', \quad \operatorname{dn} iK' = \infty.$$

Nun lassen sich K, K' vermittelst (8) durch bestimmte Integrale ausdrücken, und man erhält, wenn man v von einem Eckpunkte des Parallelogramms $0, K, K + iK', iK'$ bis zum folgenden längs der Peripherie verschiebt, also u längs

$$0, \quad \frac{1}{2}, \quad \frac{1+\omega}{2}, \quad \frac{\omega}{2}.$$

(17) $$K = \frac{1}{2}\int_0^1 \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

(18) $$iK' = \frac{1}{2}\int_1^{\frac{1}{\varkappa^2}} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

(19) $$-K = \frac{1}{2}\int_{\frac{1}{\varkappa^2}}^{\infty} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}},$$

(20) $$-iK' = \frac{1}{2}\int_{\infty}^{0} \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}}.$$

Die Werte von $\sqrt{\zeta}$, $\sqrt{1-\zeta}$, $\sqrt{1-\varkappa^2\zeta}$ sind bei diesen Integrationen durch die Formeln (4) bestimmt. Wenn aber ω rein imaginär und infolgedessen $\varkappa^2$ ein positiver echter Bruch und K, K' reell und positiv sind, so sind die Wege für v der reellen und imaginären Achse parallel, und mit Rücksicht auf die Bemerkungen am Schluß des § 25 zeigen die Formeln (4) folgendes:

In (17) sind	$\sqrt{\zeta}$,	$\sqrt{1-\zeta}$,	$\sqrt{1-\varkappa^2\zeta}$	reell	und	positiv,
„ (18) „	$\sqrt{\zeta}$,	$i\sqrt{1-\zeta}$,	$\sqrt{1-\varkappa^2\zeta}$	„	„	„
„ (19) „	$\sqrt{\zeta}$,	$i\sqrt{1-\zeta}$,	$i\sqrt{1-\varkappa^2\zeta}$	„	„	„
„ (20) „	$-i\sqrt{\zeta}$,	$\sqrt{1-\zeta}$,	$\sqrt{1-\varkappa^2\zeta}$	„	„	„

und $\sqrt{\zeta}$ hat auf keinem der Integrationswege ein Maximum oder Minimum. Es können daher K, K' durch die vier folgenden reellen Integrale mit positiver Quadratwurzel erklärt werden:

$$K = \frac{1}{2}\int_0^1 \frac{d\zeta}{\sqrt{\zeta(1-\zeta)(1-\varkappa^2\zeta)}} = \frac{1}{2}\int_{\frac{1}{\varkappa^2}}^{\infty} \frac{d\zeta}{\sqrt{\zeta(\zeta-1)(\varkappa^2\zeta-1)}},$$

$$K' = \frac{1}{2}\int_{-\infty}^{0} \frac{d\zeta}{\sqrt{-\zeta(1-\zeta)(1-\varkappa^2\zeta)}} = \frac{1}{2}\int_1^{\frac{1}{\varkappa^2}} \frac{d\zeta}{\sqrt{\zeta(\zeta-1)(1-\varkappa^2\zeta)}}.$$

§ 43. Die Jacobischen Funktionen $\Theta(v)$, $H(v)$.

Wenn man die ϑ-Funktionen der Variablen u als Funktionen von v betrachtet, so erhält man die Jacobischen Θ-Funktionen. Wir setzen

$$
(1)\qquad \begin{aligned}
\vartheta_{01}\left(\frac{v}{2K}, \omega\right) &= \Theta(v),\\
\vartheta_{11}\left(\frac{v}{2K}, \omega\right) &= H(v).
\end{aligned}
$$

Es sind dann $\Theta(v)$, $H(v)$ als Funktionen $t(v, 2K, 2K')$ zu bezeichnen, und nach § 25 ist

$$
(2)\qquad \begin{aligned}
\Theta(v) &= 1 - 2q\cos\frac{\pi v}{K} + 2q^4\cos\frac{2\pi v}{K} - 2q^9\cos\frac{3\pi v}{K} + \cdots\\
H(v) &= \quad 2q^{\frac{1}{4}}\sin\frac{\pi v}{2K} - 2q^{\frac{9}{4}}\sin\frac{3\pi v}{2K} + 2q^{\frac{25}{4}}\sin\frac{5\pi v}{2K} - \cdots
\end{aligned}
$$

$$
q = e^{-\frac{\pi K'}{K}}.
$$

Nach § 21 (8) ist

$$
(3)\qquad \begin{aligned}
H(v) &= -ie^{-\frac{\pi K'}{4K} + \frac{\pi i v}{2K}}\,\Theta(v + iK'),\\
\Theta(v) &= -ie^{-\frac{\pi K'}{4K} + \frac{\pi i v}{2K}}\,H(v + iK').
\end{aligned}
$$

Ferner:

$$
(4)\qquad \begin{aligned}
\vartheta_{00}\left(\frac{v}{2K}, \omega\right) &= \Theta(v + K),\\
\vartheta_{10}\left(\frac{v}{2K}, \omega\right) &= H(v + K),
\end{aligned}
$$

wonach, mittels der Formeln (3), (10), (15) des vorigen Paragraphen und (5), § 23:

$$
(5)\qquad \begin{gathered}
\sqrt{\varkappa} = \frac{H(K)}{\Theta(K)}, \qquad \sqrt{\varkappa'} = \frac{\Theta(0)}{\Theta(K)},\\
\Theta(K) = \sqrt{\frac{2K}{\pi}}, \quad \Theta(0) = \sqrt{\frac{2\varkappa' K}{\pi}}, \quad H(K) = \sqrt{\frac{2\varkappa K}{\pi}},\\
H'(0) = \frac{\Theta(0)\,H(K)}{\Theta(K)} = \sqrt{\frac{2\varkappa\varkappa' K}{\pi}};
\end{gathered}
$$

endlich die Darstellung der elliptischen Funktionen:

$$\frac{H(v)}{\Theta(v)} = \sqrt{\varkappa}\,\mathrm{sn}\,v,$$

(6)
$$\frac{H(v+K)}{\Theta(v)} = \sqrt{\frac{\varkappa}{\varkappa'}}\,\mathrm{cn}\,v,$$

$$\frac{\Theta(v+K)}{\Theta(v)} = \frac{1}{\sqrt{\varkappa'}}\,\mathrm{dn}\,v.$$

Die Funktionen Θ, H haben, wie aus (3) leicht folgt, die durch die folgenden Gleichungen ausgedrückte Periodizität:

(7)
$$\Theta(v+2nK) = \Theta(v),$$
$$\Theta(v+2niK') = (-1)^n e^{\frac{n^2\pi K'}{K} - \frac{\pi i n v}{K}}\,\Theta(v),$$

(8)
$$H(v+2nK) = (-1)^n H(v),$$
$$H(v+2niK') = (-1)^n e^{\frac{n^2\pi K'}{K} - \frac{\pi i n v}{K}}\,H(v).$$

Es ist bisweilen nützlich, die Gleichungen (3), (7), (8) folgendermaßen zusammenzufassen:

(9)
$$\Phi(v+niK') = i^n e^{\frac{n^2\pi i}{4}\frac{K'}{K} - \frac{\pi i n v}{2K}}\,\Psi(v),$$

worin, wenn n gerade, Φ und Ψ beide gleich Θ oder beide gleich H, wenn n ungerade, $\Phi = \Theta$, $\Psi = H$ oder $\Phi = H$, $\Psi = \Theta$ zu setzen ist.

Aus § 22 (2), (4) ergeben sich die Additionsformeln:

(10)
$$\Theta^2(0)\,\Theta(u+v)\,\Theta(u-v) = \Theta^2(u)\,\Theta^2(v) - H^2(u)\,H^2(v),$$
$$\Theta^2(0)\,H(u+v)\,H(u-v) = H^2(u)\,\Theta^2(v) - \Theta^2(u)\,H^2(v),$$

wofür man auch schreiben kann:

(11)
$$\Theta^2(0)\,\Theta(u+v)\,\Theta(u-v) = \Theta^2(u)\,\Theta^2(v)\,(1 - \varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v),$$
$$\Theta^2(0)\,H(u+v)\,H(u-v) = \Theta^2(u)\,\Theta^2(v)\,\varkappa\,(\mathrm{sn}^2 u - \mathrm{sn}^2 v).$$

Wir gehen nun dazu über, die Sätze über die ϑ-Funktionen auf die elliptischen Funktionen zu übertragen und beginnen mit dem Additionstheorem.

§ 44. Additionstheorem der elliptischen Funktionen.

Aus den vier ϑ-Funktionen lassen sich im ganzen zwölf Quotienten bilden, die nach § 42 durch elliptische Funktionen ausdrückbar sind. Bildet man diese Quotienten für das Argument $u + v$, so kann man diese nach § 22 durch ϑ-Funktionen von u und von v einzeln, also auch durch die entsprechenden elliptischen Funktionen darstellen, und zwar immer so, daß der Nenner

nur Quadrate von ϑ enthält, also rational durch $\mathrm{sn}^2 u$, $\mathrm{sn}^2 v$ ausgedrückt wird. Nehmen wir, um ein Beispiel durchzuführen, die Formel (5), § 22, und dividieren sie einmal durch (1) und dann durch (4) (indem wir das erste Mal in (5) v in $-v$ verwandeln), so folgt:

$$\frac{\vartheta_{01}\vartheta_{10}}{\vartheta_{00}^2}\frac{\vartheta_{11}(u+v)}{\vartheta_{00}(u+v)}$$
$$=\frac{\vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{10}(v)+\vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{11}(v)}{\vartheta_{00}^2(u)\vartheta_{00}^2(v)+\vartheta_{11}^2(u)\vartheta_{11}^2(v)},$$
$$\frac{\vartheta_{10}}{\vartheta_{01}}\frac{\vartheta_{00}(u+v)}{\vartheta_{11}(u+v)}$$
$$=\frac{\vartheta_{00}(u)\vartheta_{11}(u)\vartheta_{01}(v)\vartheta_{10}(v)-\vartheta_{01}(u)\vartheta_{10}(u)\vartheta_{00}(v)\vartheta_{11}(v)}{\vartheta_{11}^2(u)\vartheta_{01}^2(v)-\vartheta_{01}^2(u)\vartheta_{11}^2(v)},$$

und wenn man u, v ersetzt durch $u:2K$, $v:2K$, so kann man nach § 42 (10) alles durch elliptische Funktionen ausdrücken. Man erhält so

$$(1)\qquad \frac{\mathrm{sn}(u+v)}{\mathrm{dn}(u+v)}=\frac{\mathrm{dn}\,u\,\mathrm{sn}\,u\,\mathrm{cn}\,v+\mathrm{dn}\,v\,\mathrm{sn}\,v\,\mathrm{cn}\,u}{\mathrm{dn}^2 u\,\mathrm{dn}^2 v+\varkappa^2\varkappa'^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(2)\qquad \frac{\mathrm{dn}(u+v)}{\mathrm{sn}(u+v)}=\frac{\mathrm{dn}\,u\,\mathrm{sn}\,u\,\mathrm{cn}\,v-\mathrm{dn}\,v\,\mathrm{sn}\,v\,\mathrm{cn}\,u}{\mathrm{sn}^2 u-\mathrm{sn}^2 v}.$$

Auf demselben Wege erhält man aus den Formeln (6), (3), (4); (7), (2), (4); (8), (2), (3); (9), (1), (2); (10), (1), (3) des § 22:

$$(3)\qquad \frac{\mathrm{sn}(u+v)}{\mathrm{cn}(u+v)}=\frac{\mathrm{cn}\,u\,\mathrm{sn}\,u\,\mathrm{dn}\,v+\mathrm{cn}\,v\,\mathrm{sn}\,v\,\mathrm{dn}\,u}{\mathrm{cn}^2 u\,\mathrm{cn}^2 v-\varkappa'^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(4)\qquad \frac{\mathrm{cn}(u+v)}{\mathrm{sn}(u+v)}=\frac{\mathrm{cn}\,u\,\mathrm{sn}\,u\,\mathrm{dn}\,v-\mathrm{cn}\,v\,\mathrm{sn}\,v\,\mathrm{dn}\,u}{\mathrm{sn}^2 u-\mathrm{sn}^2 v},$$

$$(5)\qquad \mathrm{sn}(u+v)=\frac{\mathrm{sn}\,u\,\mathrm{cn}\,v\,\mathrm{dn}\,v+\mathrm{sn}\,v\,\mathrm{cn}\,u\,\mathrm{dn}\,u}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(6)\qquad \frac{1}{\mathrm{sn}(u+v)}=\frac{\mathrm{sn}\,u\,\mathrm{cn}\,v\,\mathrm{dn}\,v-\mathrm{sn}\,v\,\mathrm{cn}\,u\,\mathrm{dn}\,u}{\mathrm{sn}^2 u-\mathrm{sn}^2 v},$$

$$(7)\qquad \mathrm{cn}(u+v)=\frac{\mathrm{cn}\,u\,\mathrm{cn}\,v-\mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{dn}\,u\,\mathrm{dn}\,v}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(8)\qquad \frac{1}{\mathrm{cn}(u+v)}=\frac{\mathrm{cn}\,u\,\mathrm{cn}\,v+\mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{dn}\,u\,\mathrm{dn}\,v}{\mathrm{cn}^2 u\,\mathrm{cn}^2 v-\varkappa'^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(9)\qquad \mathrm{dn}(u+v)=\frac{\mathrm{dn}\,u\,\mathrm{dn}\,v-\varkappa^2\,\mathrm{sn}\,u\,\mathrm{sn}\,v\,\mathrm{cn}\,u\,\mathrm{cn}\,v}{1-\varkappa^2\,\mathrm{sn}^2 u\,\mathrm{sn}^2 v},$$

$$(10)\qquad \frac{1}{\operatorname{dn}(u+v)} = \frac{\operatorname{dn}u \operatorname{dn}v + \varkappa^2 \operatorname{sn}u \operatorname{sn}v \operatorname{cn}u \operatorname{cn}v}{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v},$$

$$(11)\qquad \frac{\operatorname{dn}(u+v)}{\operatorname{cn}(u+v)} = \frac{\operatorname{dn}u \operatorname{dn}v \operatorname{cn}u \operatorname{cn}v + \varkappa'^2 \operatorname{sn}u \operatorname{sn}v}{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v},$$

$$(12)\qquad \frac{\operatorname{cn}(u+v)}{\operatorname{dn}(u+v)} = \frac{\operatorname{dn}u \operatorname{dn}v \operatorname{cn}u \operatorname{cn}v - \varkappa'^2 \operatorname{sn}u \operatorname{sn}v}{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}.$$

Man kann noch mannigfache andere Formeln auf dieselbe Weise herleiten, unter denen wir die folgenden drei anführen, die sich durch Division von § 22 (4), (3), (1) durch (2) ergeben.

$$(13)\qquad \operatorname{sn}(u+v) \operatorname{sn}(u-v) = \frac{\operatorname{sn}^2 u - \operatorname{sn}^2 v}{1 - \varkappa^2 \operatorname{ns}^2 u \operatorname{sn}^2 v},$$

$$(14)\qquad \operatorname{cn}(u+v) \operatorname{cn}(u-v) = \frac{\operatorname{cn}^2 u \operatorname{cn}^2 v - \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v},$$

$$(15)\qquad \operatorname{dn}(u+v) \operatorname{dn}(u-v) = \frac{\operatorname{dn}^2 u \operatorname{dn}^2 v + \varkappa^2 \varkappa'^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}.$$

Die wichtigsten unter diesen Formeln sind (5), (7), (9), aus denen sich, wenn auch durch weitläufige Rechnungen, die übrigen alle herleiten lassen. Der Übersicht halber setzen wir sie noch einmal her:

$$(16)\qquad \begin{aligned} \operatorname{sn}(u+v) &= \frac{\operatorname{sn}u \operatorname{cn}v \operatorname{dn}v + \operatorname{sn}v \operatorname{cn}u \operatorname{dn}u}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \\ \operatorname{cn}(u+v) &= \frac{\operatorname{cn}u \operatorname{cn}v - \operatorname{sn}u \operatorname{sn}v \operatorname{dn}u \operatorname{dn}v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}, \\ \operatorname{dn}(u+v) &= \frac{\operatorname{dn}u \operatorname{dn}v - \varkappa^2 \operatorname{sn}u \operatorname{sn}v \operatorname{cn}u \operatorname{cn}v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}. \end{aligned}$$

Indem man je zwei dieser Gleichungen kombiniert, kann man ihnen unter anderen die Formen geben:

$$(17)\qquad \begin{aligned} &\operatorname{cn}(u+v) \operatorname{dn}u \operatorname{dn}v - \operatorname{dn}(u+v) \operatorname{cn}u \operatorname{cn}v = -\varkappa'^2 \operatorname{sn}u \operatorname{sn}v \\ &\operatorname{dn}(u+v) \operatorname{sn}u \operatorname{cn}v - \operatorname{sn}(u+v) \operatorname{dn}u = -\operatorname{cn}u \operatorname{sn}v, \\ &\operatorname{sn}(u+v) \operatorname{cn}u - \operatorname{cn}(u+v) \operatorname{sn}u \operatorname{dn}v = \operatorname{dn}u \operatorname{sn}v, \\ &\operatorname{cn}(u+v) \operatorname{cn}u + \operatorname{sn}(u+v) \operatorname{sn}u \operatorname{dn}v = \operatorname{cn}v. \end{aligned}$$

Wir wenden die Formeln (16) zunächst an zur Feststellung der Periodizität der elliptischen Funktionen, die sich natürlich auch aus § 21 herleiten läßt. Setzt man in (16) $v = \pm K$, $v = K + iK'$, so folgt aus § 42 (16):

$$
\begin{aligned}
&\operatorname{sn}(u \pm K) = \pm \frac{\operatorname{cn} u}{\operatorname{dn} u}, \\
(18) \qquad &\operatorname{cn}(u \pm K) = \mp \frac{\varkappa' \operatorname{sn} u}{\operatorname{dn} u}, \\
&\operatorname{dn}(u \pm K) = \frac{\varkappa'}{\operatorname{dn} u},
\end{aligned}
$$

$$
\begin{aligned}
&\operatorname{sn}(u + K + iK') = \frac{1}{\varkappa} \frac{\operatorname{dn} u}{\operatorname{cn} u}, \\
(19) \qquad &\operatorname{cn}(u + K + iK') = \frac{i\varkappa'}{\varkappa} \frac{1}{\operatorname{cn} u}, \\
&\operatorname{dn}(u + K + iK') = \frac{i\varkappa' \operatorname{sn} u}{\operatorname{cn} u},
\end{aligned}
$$

und wenn man in (19) u in $u - K$ verwandelt:

$$
\begin{aligned}
&\operatorname{sn}(u + iK') = \frac{1}{\varkappa} \frac{1}{\operatorname{sn} u}, \\
(20) \qquad &\operatorname{cn}(u + iK') = -\frac{i}{\varkappa} \frac{\operatorname{dn} u}{\operatorname{sn} u}, \\
&\operatorname{dn}(u + iK') = -i \frac{\operatorname{cn} u}{\operatorname{sn} u}.
\end{aligned}
$$

Die Formeln (20) zeigen, daß die drei Funktionen $\operatorname{sn} u$, $\operatorname{cn} u$, $\operatorname{dn} u$ für $u = iK'$ unendlich werden. Bildet man die Quotienten je zweier von ihnen, so folgt:

$$
(21) \qquad \left.
\begin{aligned}
&\lim \frac{\operatorname{sn} u}{\operatorname{cn} u} = i \\
&\lim \frac{\operatorname{sn} u}{\operatorname{dn} u} = i
\end{aligned}
\right\} \quad \text{für } u = iK'.
$$

Mit Hilfe der Relationen (18), (19), (20) kann man aus jeder Additionsformel drei andere ableiten, indem man u durch $u + K$, $u + K + iK'$, $u + iK'$ ersetzt, also die Vertauschungen macht, die in folgender Tabelle zusammengestellt sind:

$\operatorname{sn} u$,	$\operatorname{cn} u$,	$\operatorname{dn} u$,
$\dfrac{\operatorname{cn} u}{\operatorname{dn} u}$,	$\dfrac{-\varkappa' \operatorname{sn} u}{\operatorname{dn} u}$,	$\dfrac{\varkappa'}{\operatorname{dn} u}$,
$\dfrac{1}{\varkappa} \dfrac{\operatorname{dn} u}{\operatorname{cn} u}$,	$\dfrac{i\varkappa'}{\varkappa \operatorname{cn} u}$,	$\dfrac{i\varkappa' \operatorname{sn} u}{\operatorname{cn} u}$,
$\dfrac{1}{\varkappa \operatorname{sn} u}$,	$\dfrac{-i \operatorname{dn} u}{\varkappa \operatorname{sn} u}$,	$\dfrac{-i \operatorname{cn} u}{\operatorname{sn} u}$,

und dieselben Vertauschungen auch auf $\operatorname{sn}(u \pm v)$, $\operatorname{cn}(u \pm v)$, $\operatorname{dn}(u \pm v)$ anwendet. So ergeben sich z. B. die zwölf Formeln (1) bis (12) aus den drei Formeln (16).

Wendet man diese Vertauschungen auf die Relationen (18), (19), (20) selber an, so ergibt sich:

$$
\begin{aligned}
&\operatorname{sn}(u+2K) = -\operatorname{sn} u, && \operatorname{sn}(u+2iK') = \operatorname{sn} u,\\
(22)\qquad &\operatorname{cn}(u+2K) = -\operatorname{cn} u, && \operatorname{cn}(u+2iK') = -\operatorname{cn} u,\\
&\operatorname{dn}(u+2K) = \operatorname{dn} u, && \operatorname{dn}(u+2iK') = -\operatorname{dn} u.
\end{aligned}
$$

Die gemeinschaftlichen Perioden dieser drei Funktionen sind also $4K$, $4iK'$; außerdem hat aber $\operatorname{sn} u$ die Periode $2iK'$, $\operatorname{dn} u$ die Periode $2K$, $\operatorname{cn} u$ die Periode $2K + 2iK'$.

Wir geben nur dem Satz über Θ-Funktionen (§ 21) einen anderen Ausdruck, indem wir den folgenden Satz aussprechen:

Jede doppelt periodische Funktion von v mit den Perioden $2K$, $2iK'$ (die überall den Charakter einer rationalen Funktion hat) ist, wenn sie eine gerade Funktion ist, eine rationale Funktion von $\operatorname{sn}^2 v$, und wenn sie eine ungerade Funktion ist, das Produkt von $\operatorname{sn} v \operatorname{cn} v \operatorname{dn} v$ mit einer rationalen Funktion von $\operatorname{sn}^2 v$.

So kann man jeden Satz, der sich auf homogene Funktionen nullter Ordnung von ϑ-Funktionen bezieht, in einen Satz über elliptische Funktionen verwandeln, und erhält daraus wieder entsprechende Sätze über elliptische Integrale. Man erkennt sofort, daß die Additionsformeln (16) keine anderen sind, als die Formeln (17) des § 13 im ersten Abschnitt. In derselben Weise liefert uns die Transformationstheorie der ϑ-Funktionen eine Lösung des Jacobischen Transformationsproblems der elliptischen Integrale, wie wir es im § 8 dargelegt haben.

Wir wollen dies an den beiden Haupttransformationen zweiter Ordnung nachweisen, die wir im § 32 ebenso wie im § 9 als Gausssche und Landensche Transformation bezeichnet haben. Nach § 32 ist für die Gausssche Transformation

$$
(23)\qquad \frac{\vartheta_{10}\left(0, \frac{\omega}{2}\right) \vartheta_{11}\left(u, \frac{\omega}{2}\right)}{\vartheta_{00}\left(0, \frac{\omega}{2}\right) \vartheta_{01}\left(u, \frac{\omega}{2}\right)} = \frac{2\,\vartheta_{01}(u)\,\vartheta_{11}(u)}{\vartheta_{01}^2(u) + \vartheta_{11}^2(u)},
$$

$$
(24)\qquad \frac{\vartheta_{10}\left(0, \frac{\omega}{2}\right)^2}{\vartheta_{00}\left(0, \frac{\omega}{2}\right)^2} = \frac{2\,\vartheta_{10}\vartheta_{00}}{\vartheta_{00}^2 + \vartheta_{10}^2} = \frac{2\sqrt{\varkappa}}{1+\varkappa},
$$

$$(25) \qquad \vartheta_{00}\left(0, \frac{\omega}{2}\right)^2 = \vartheta_{00}^2 + \vartheta_{10}^2 = (1 + \varkappa)\,\vartheta_{00}^2.$$

Nach § 42 erhalten wir also eine Beziehung zwischen elliptischen Funktionen mit zwei verschiedenen Moduln, und es ist, wenn λ, L, L' aus $\varkappa$, K, K' durch die Vertauschung $\left(\omega, \frac{\omega}{2}\right)$ hervorgehen, nach (23), (24), (25)

$$(26) \qquad \lambda = \frac{2\sqrt{\varkappa}}{1+\varkappa}, \quad L = (1+\varkappa)K, \quad L' = (1+\varkappa)K'$$

$$(27) \qquad \operatorname{sn}[(1+\varkappa)v, \lambda] = \frac{(1+\varkappa)\operatorname{sn} v}{1+\varkappa\operatorname{sn}^2 v},$$

wenn der Deutlichkeit halber der Modul unter dem Funktionszeichen sn als zweites Argument mit aufgeführt ist.

Für die Landensche Transformation ist

$$\frac{\vartheta_{11}(2u, 2\omega)}{\vartheta_{01}(2u, 2\omega)} = \frac{\vartheta_{10}(u)\,\vartheta_{11}(u)}{\vartheta_{00}(u)\,\vartheta_{01}(u)},$$

$$\frac{\vartheta_{01}(0, 2\omega)^2}{\vartheta_{00}(0, 2\omega)^2} = \frac{2\,\vartheta_{00}\,\vartheta_{01}}{\vartheta_{00}^2 + \vartheta_{01}^2} = \frac{2\sqrt{\varkappa'}}{1+\varkappa'},$$

$$2\,\vartheta_{00}^2(0, 2\omega) = (1+\varkappa')\,\vartheta_{00}^2,$$

daraus, wenn λ, λ', L, L' durch die Vertauschung $(\omega, 2\omega)$ aus $\varkappa$, $\varkappa'$ K, K' entstehen:

$$(28) \qquad \lambda' = \frac{2\sqrt{\varkappa'}}{1+\varkappa'}, \qquad \sqrt{\lambda} = \frac{\varkappa}{1+\varkappa'}, \qquad \lambda = \frac{1-\varkappa'}{1+\varkappa'},$$

$$2L = (1+\varkappa')K, \qquad L' = (1+\varkappa')K',$$

$$(29) \qquad \operatorname{sn}[(1+\varkappa')v, \lambda] = \frac{(1+\varkappa')\operatorname{sn} v \operatorname{cn} v}{\operatorname{dn} v},$$

und in (26) bis (29) erkennt man nach § 42 die Formeln (2) und (4) des § 9.

§ 45. Die lineare Transformation der elliptischen Funktionen.

Die Einwirkung der linearen Transformation auf die elliptischen Funktionen übersieht man am besten aus der Darstellung durch die σ-Funktionen. Man erhält aus (4) oder (10), § 42 und den Formeln (4), (6) des § 37:

(1)
$$\frac{\omega_1}{2K}\operatorname{sn}\frac{2Ku}{\omega_1} = \frac{\sigma(u)}{\sigma_{01}(u)},\quad \operatorname{cn}\frac{2Ku}{\omega_1} = \frac{\sigma_{10}(u)}{\sigma_{01}(u)},\quad \operatorname{dn}\frac{2Ku}{\omega_1} = \frac{\sigma_{00}(u)}{\sigma_{01}(u)},$$

oder auch, indem man von der Homogeneität der σ-Funktion Gebrauch macht [§ 37 (8)]:

(2)
$$\operatorname{sn} v = \frac{\sigma(v, 2K, 2iK')}{\sigma_{01}(v, 2K, 2iK')},\quad \operatorname{cn} v = \frac{\sigma_{10}(v, 2K, 2iK')}{\sigma_{01}(v, 2K, 2iK')},\quad \operatorname{dn} v = \frac{\sigma_{00}(v, 2K, 2iK')}{\sigma_{01}(v, 2K, 2iK')}.$$

Die auf der rechten Seite von (2) vorkommenden σ-Funktionen hängen nur von den beiden Variablen v, ω ab und es kommt zunächst darauf an, die Änderung dieser Funktionen bei Anwendung der Fundamentaltransformationen

$$(\omega, \omega + 1), \qquad \left(\omega, -\frac{1}{\omega}\right)$$

zu bestimmen. Wegen

$$\pi\vartheta_{00}^2 = 2K, \qquad 2iK' = 2\omega K$$

erhält man aus § 31 (6) und (11) die entsprechenden Änderungen:

ω,	$2K$,	$2iK'$,	$\varkappa$,	$\varkappa'$,
$\omega + 1$,	$2\varkappa' K$,	$2\varkappa'(K + iK')$,	$\frac{i\varkappa}{\varkappa'}$,	$\frac{1}{\varkappa'}$,
$-\frac{1}{\omega}$,	$2K'$,	$2iK$,	$\varkappa'$,	$\varkappa$.

Setzt man für den Augenblick:

$$f(v, \omega) = \sigma(v, 2K, 2iK'),$$

so ergibt sich:

$$\begin{aligned} f(v, \omega + 1) &= \sigma[v, 2\varkappa' K, 2\varkappa'(K + iK')] \\ &= \sigma(v, 2\varkappa' K, 2\varkappa' iK') \text{ [nach § 35 (7)]} \\ &= \varkappa'\sigma\left(\frac{v}{\varkappa'}, 2K, 2iK'\right) \text{ [nach § 37 (8)]}, \\ f\left(v, -\frac{1}{\omega}\right) &= \sigma(v, 2K', 2iK) \\ &= \sigma(v, -2iK, 2K') \text{ [nach § 35 (7)]} \\ &= -i\sigma(iv, 2K, 2iK') \text{ [nach § 37 (8)]}, \end{aligned}$$

und wenn man für die drei übrigen σ-Funktionen das entsprechende macht und § 36 (7) berücksichtigt, so erhält man die folgenden zusammengehörigen Vertauschungen:

$$
(3) \qquad
\begin{array}{lllll}
\omega, & \sigma(v), & \sigma_{00}(v), & \sigma_{01}(v), & \sigma_{10}(v), \\
\omega+1, & \varkappa'\sigma\left(\frac{v}{\varkappa'}\right), & \sigma_{01}\left(\frac{v}{\varkappa'}\right), & \sigma_{00}\left(\frac{v}{\varkappa'}\right), & \sigma_{10}\left(\frac{v}{\varkappa'}\right), \\
-\frac{1}{\omega}, & -i\sigma(iv), & \sigma_{00}(iv), & \sigma_{10}(iv), & \sigma_{01}(iv),
\end{array}
$$

worin die Perioden $2K$, $2iK'$ sind. Daraus folgen nach (2) die beiden ersten linearen Transformationen der elliptischen Funktionen:

$$
(4) \qquad
\begin{aligned}
\operatorname{sn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) &= \varkappa' \frac{\operatorname{sn} v}{\operatorname{dn} v}, \\
\operatorname{cn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) &= \frac{\operatorname{cn} v}{\operatorname{dn} v}, \\
\operatorname{dn}\left(\varkappa' v, \frac{i\varkappa}{\varkappa'}\right) &= \frac{1}{\operatorname{dn} v}.
\end{aligned}
$$

$$
(5) \qquad
\begin{aligned}
\operatorname{sn}(iv, \varkappa') &= i\frac{\operatorname{sn} v}{\operatorname{cn} v}, \\
\operatorname{cn}(iv, \varkappa') &= \frac{1}{\operatorname{cn} v}, \\
\operatorname{dn}(iv, \varkappa') &= \frac{\operatorname{dn} v}{\operatorname{cn} v}.
\end{aligned}
$$

Die erste Formel (5) zeigt nach § 44 (21), daß $\operatorname{sn}(v, \varkappa') = 1$ wird, wenn $v = K'$ wird. Daraus ergibt sich nach § 42 (17) die zweite häufig gebrauchte Darstellung für K':

$$
(6) \qquad K' = \frac{1}{2}\int_0^1 \frac{d\xi}{\sqrt{\xi(1-\xi)(1-\varkappa'^2\xi)}}.
$$

Aus (4), (5) erhält man die übrigen Fälle der linearen Transformation durch wiederholte Anwendung. Setzt man in (4) iv, $\varkappa'$ an Stelle von v, $\varkappa$ und wendet (5) an, so folgt:

$$
(7) \qquad
\begin{aligned}
\operatorname{sn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) &= i\varkappa \frac{\operatorname{sn} v}{\operatorname{dn} v}, \\
\operatorname{cn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) &= \frac{1}{\operatorname{dn} v}, \\
\operatorname{dn}\left(i\varkappa v, \frac{i\varkappa'}{\varkappa}\right) &= \frac{\operatorname{cn} v}{\operatorname{dn} v}.
\end{aligned}
$$

Ersetzt man umgekehrt in (5) v, $\varkappa$, $\varkappa'$ durch $\varkappa' v$, $\frac{i\varkappa}{\varkappa'}$, $\frac{1}{\varkappa'}$ und wendet (4) an, so folgt:

$$\text{(8)}\qquad \begin{aligned} \operatorname{sn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) &= i\varkappa' \frac{\operatorname{sn} v}{\operatorname{cn} v}, \\ \operatorname{cn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) &= \frac{\operatorname{dn} v}{\operatorname{cn} v}, \\ \operatorname{dn}\left(i\varkappa' v, \frac{1}{\varkappa'}\right) &= \frac{1}{\operatorname{cn} v}. \end{aligned}$$

Ersetzt man hierin wieder v durch iv und $\varkappa$, $\varkappa'$ durch $\varkappa'$, $\varkappa$ und wendet (5) an, so findet man:

$$\text{(9)}\qquad \begin{aligned} \operatorname{sn}\left(\varkappa v, \frac{1}{\varkappa}\right) &= \varkappa \operatorname{sn} v, \\ \operatorname{cn}\left(\varkappa v, \frac{1}{\varkappa}\right) &= \operatorname{dn} v, \\ \operatorname{dn}\left(\varkappa v, \frac{1}{\varkappa}\right) &= \operatorname{cn} v, \end{aligned}$$

womit die sechs Klassen der linearen Transformationen erschöpft sind, da eine noch häufigere Wiederholung zu keinen neuen Formeln Anlaß gibt.

§ 46. Die Weierstrasssche $\wp$-Funktion.

Die linearen Transformationen der elliptischen Funktionen legen es nahe, eine elliptische Funktion zu suchen, die, wie die σ-Funktion selbst, den linearen Transformationen gegenüber unveränderlich ist. Um eine solche Funktion zu bilden, setzen wir zunächst die Gleichungen (1) des vorigen Paragraphen in folgende Form:

$$\text{(1)}\qquad \begin{aligned} \frac{\sigma_{10}(u)}{\sigma(u)} &= \frac{2K}{\omega_1}\frac{\operatorname{cn} v}{\operatorname{sn} v}, \\ \frac{\sigma_{00}(u)}{\sigma(u)} &= \frac{2K}{\omega_1}\frac{\operatorname{dn} v}{\operatorname{sn} v}, \\ \frac{\sigma_{01}(u)}{\sigma(u)} &= \frac{2K}{\omega_1}\frac{1}{\operatorname{sn} v}, \end{aligned}$$

worin zur Abkürzung

$$\text{(2)}\qquad v = \frac{2Ku}{\omega_1}$$

gesetzt ist. Hieraus schließt man mit Hilfe der Relationen

$$\operatorname{cn}^2 v = 1 - \operatorname{sn}^2 v, \qquad \operatorname{dn}^2 v = 1 - \varkappa^2 \operatorname{sn}^2 v,$$

$$\frac{\sigma_{01}^2(u)}{\sigma^2(u)} - \frac{\sigma_{10}^2(u)}{\sigma^2(u)} = \frac{4K^2}{\omega_1^2},$$

$$\frac{\sigma_{01}^2(u)}{\sigma^2(u)} - \frac{\sigma_{00}^2(u)}{\sigma^2(u)} = \frac{4K^2}{\omega_1^2}\varkappa^2.$$

Es lassen sich daher drei von u unabhängige (also nur von ω_1, ω_2 abhängige) Größen e_1, e_2, e_3 so bestimmen, daß

$$\frac{\sigma_{10}^2(u)}{\sigma^2(u)} + e_1 = \frac{\sigma_{00}^2(u)}{\sigma^2(u)} + e_2 = \frac{\sigma_{01}^2(u)}{\sigma^2(u)} + e_3 = \wp(u), \tag{3}$$

worin $\wp(u)$ eine durch (3) neu definierte, doppelt periodische Funktion ist. Die Größen e_1, e_2, e_3 können irgend welche sein, wenn sie nur den Bedingungen

$$e_1 - e_3 = \frac{4K^2}{\omega_1^2}, \quad e_2 - e_3 = \frac{4K^2}{\omega_1^2}\varkappa^2 \tag{4}$$

genügen. Es steht uns also frei, zur völligen Bestimmung derselben noch die Bedingung

$$e_1 + e_2 + e_3 = 0 \tag{5}$$

hinzuzufügen. Dann ergeben sich für e_1, e_2, e_3 folgende Ausdrücke:

$$\begin{aligned} e_1 &= \frac{4K^2}{\omega_1^2}\,\frac{1+\varkappa'^2}{3}, \\ e_2 &= -\frac{4K^2}{\omega_1^2}\,\frac{\varkappa'^2-\varkappa^2}{3}, \\ e_3 &= -\frac{4K^2}{\omega_1^2}\,\frac{1+\varkappa^2}{3}. \end{aligned} \tag{6}$$

Die Funktion $\wp(u)$, welche die Perioden ω_1, ω_2 besitzt, wird hiernach durch (1) ausgedrückt:

$$\wp(u) = \frac{4K^2}{\omega_1^2}\left(\frac{1}{\operatorname{sn}^2 v} - \frac{1+\varkappa^2}{3}\right). \tag{7}$$

Die Funktion $\wp(u)$ hat die gewünschte Eigenschaft der Unveränderlichkeit bei linearen Transformationen, wie man aus dem Ausdruck

$$\wp(u) = \frac{1}{3}\,\frac{\sigma_{00}^2(u) + \sigma_{01}^2(u) + \sigma_{10}^2(u)}{\sigma^2(u)} \tag{8}$$

erkennt.

Infolge von (3) vertauschen sich die e_1, e_2, e_3 bei einer linearen Transformation in derselben Weise wie die σ_{10}, σ_{00}, σ_{01}; eine symmetrische Funktion derselben ist daher bei einer linearen Trans-

formation ungeändert und wird eine Invariante genannt. Es gibt deren zwei fundamentale, die wir mit g_2, g_3 bezeichnen:

$$(9) \qquad g_2 = -4(e_2 e_3 + e_3 e_1 + e_1 e_2) = 2(e_1^2 + e_2^2 + e_3^2) = \frac{64}{3}\frac{K^4}{\omega_1^4}(1 - \varkappa^2 \varkappa'^2),$$

$$(10) \qquad g_3 = 4 e_1 e_2 e_3 = \frac{2^8}{27}\frac{K^6}{\omega_1^6}(2 + \varkappa^2 \varkappa'^2)(\varkappa'^2 - \varkappa^2),$$

und wir fügen noch die unter dem Namen der Diskriminante bekannte Funktion bei:

$$(11) \qquad G = (e_2 - e_3)^2 (e_3 - e_1)^2 (e_1 - e_2)^2 = \frac{1}{16}(g_2^3 - 27 g_3^2) = \frac{(2K)^{12}}{\omega_1^{12}} \varkappa^4 \varkappa'^4,$$

wofür nach § 43 (3), (15) und § 34 (2) auch gesetzt werden kann:

$$(12) \qquad G = \frac{2^8 \pi^{12} \eta(\omega)^{24}}{\omega_1^{12}}.$$

$\wp(u)$, g_2, g_3, G sind homogene Funktionen, wie folgende Relationen zeigen, worin λ ein willkürlicher Faktor ist.

$$(13) \qquad \begin{aligned} \wp(\lambda u, \lambda\omega_1, \lambda\omega_2) &= \lambda^{-2} \wp(u, \omega_1, \omega_2), \\ \wp'(\lambda u, \lambda\omega_1, \lambda\omega_2) &= \lambda^{-3} \wp'(u, \omega_1, \omega_2), \\ g_2(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-4} g_2(\omega_1, \omega_2), \\ g_3(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-6} g_3(\omega_1, \omega_2), \\ G(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-12} G(\omega_1, \omega_2). \end{aligned}$$

Setzen wir, wie in § 45 (2)

$$\omega_1 = 2K, \qquad \omega_2 = 2iK';$$

so wird

$$(14) \qquad \begin{gathered} e_1 = \frac{1 + \varkappa'^2}{3}, \quad e_2 = -\frac{\varkappa'^2 - \varkappa^2}{3}, \quad e_3 = -\frac{1 + \varkappa^2}{3}, \\ g_2 = \frac{4}{3}(1 - \varkappa^2 \varkappa'^2), \quad g_3 = \frac{4}{27}(\varkappa'^2 - \varkappa^2)(2 + \varkappa^2 \varkappa'^2), \\ G = \varkappa^4 \varkappa'^4. \end{gathered}$$

Wenn wir ω_1 aus den allgemeinen Ausdrücken (9), (10), (11) für g_2, g_3, G eliminieren, so erhalten wir homogene Funktionen nullter Ordnung, also Funktionen von ω allein, die bei linearen Transformationen ungeändert bleiben. Solche Funktionen sind $g_2^3 : G$, $g_3^2 : G$. Wir heben unter diesen Funktionen, die sich alle aufeinander zurückführen lassen, eine hervor, die wir mit

$j(\omega)$ bezeichnen und schlechtweg die Invariante nennen und so definieren:

(15) $$j(\omega) = 2^8 \frac{(1 - \varkappa^2 \varkappa'^2)^3}{\varkappa^4 \varkappa'^4},$$

woraus wir erhalten:

$$\frac{4 . 27 g_2^3}{G} = j(\omega),$$

(16) $$\frac{4 . 27 . 27 g_3^2}{G} = j(\omega) - 27 . 64 = \frac{64 . (2 + \varkappa^2 \varkappa'^2)^2 (\varkappa'^2 - \varkappa^2)^2}{\varkappa^4 \varkappa'^4}.$$

Als Funktion von $\varkappa^2$ betrachtet, hat die Funktion $j(\omega)$ die Eigenschaft, ungeändert zu bleiben, wenn $\varkappa^2$ durch einen der sechs Werte

$$\varkappa^2, \quad \varkappa'^2, \quad \frac{1}{\varkappa^2}, \quad \frac{1}{\varkappa'^2}, \quad -\frac{\varkappa^2}{\varkappa'^2}, \quad -\frac{\varkappa'^2}{\varkappa^2}$$

ersetzt wird.

Wenn wir nach (7) den Differentialquotienten der Funktion $\wp(u)$ bilden, so erhalten wir

(17) $$\wp'(u) = -\frac{16 K^3}{\omega_1^3} \frac{\operatorname{cn} v \operatorname{dn} v}{\operatorname{sn}^3 v} = -2 \frac{\sigma_{00}(u) \sigma_{10}(u) \sigma_{01}(u)}{\sigma(u)^3}$$

und daraus nach (3):

(18) $$\begin{aligned} \wp'(u)^2 &= 4[\wp(u) - e_1][\wp(u) - e_2][\wp(u) - e_3] \\ &= 4 \wp(u)^3 - g_2 \wp(u) - g_3, \end{aligned}$$

oder endlich

(19) $$du = \frac{d \wp}{\sqrt{4 \wp^3 - g_2 \wp - g_3}},$$

woraus man ersieht, daß die Funktion $\wp(u)$ in derselben Beziehung zur Weierstrassschen Normalform des elliptischen Differentials steht, wie die Funktion $\operatorname{sn} v$ zu der Legendreschen.

§ 47. Die elliptischen Transzendenten zweiter Gattung.

Jacobi hat als Transzendente zweiter Gattung die Funktion

(1) $$Z(v) = \frac{\Theta'(v)}{\Theta(v)} = \frac{d \log \Theta(v)}{dv}$$

eingeführt. Die Beziehung dieser Funktion zu den elliptischen Integralen zweiter Gattung ergibt sich aus der Formel (16) des § 23, wobei gleich bemerkt sei, daß ganz ähnliche Betrachtungen an die dortigen Formeln (15), (17), (18) anzuknüpfen wären, die aber nicht zu wesentlich neuen Resultaten führen.

Setzen wir dort $v:2K$ an Stelle von v, so ergibt sich aus § 42 und 43:

(2) $$\frac{d^2 \log \Theta(v)}{dv^2} = \frac{1}{4K^2}\frac{\vartheta''_{01}}{\vartheta_{01}} - \varkappa^2 \operatorname{sn}^2 v$$
$$= \frac{1}{4K^2}\frac{\vartheta''_{01}}{\vartheta_{01}} - 1 + \operatorname{dn}^2 v.$$

Wir setzen

(3) $$1 - \frac{\vartheta''_{01}}{4K^2\vartheta_{01}} = \frac{E}{K},$$

und erhalten durch Integration von (2)

$$\frac{d \log \Theta(v)}{dv} = Z(v) = -\frac{E}{K}v + \int_0^v \operatorname{dn}^2 v\, dv,$$

oder indem wir

(4) $$E(v) = \int_0^v \operatorname{dn}^2 v\, dv$$

setzen:

(5) $$Z(v) = E(v) - \frac{E}{K}v, \quad \frac{dZ(v)}{dv} = \operatorname{dn}^2 v - \frac{E}{K}.$$

Die Funktionen $\Theta(v)$ und $\Theta(v+K)$ sind gerade Funktionen und daher ist $\Theta'(0)$ und $\Theta'(K) = 0$. Wenn wir also in (5) $v = K$ setzen, so folgt:

(6) $$E = \int_0^K \operatorname{dn}^2 v\, dv.$$

Führt man noch für dv das Differential

$$\frac{1}{2}\frac{d\xi}{\sqrt{\xi(1-\xi)(1-\varkappa^2\xi)}}$$

ein [§ 42 (8)], so erhält man für $E(v)$ ein elliptisches Integral zweiter Gattung (§ 11):

(7) $$E(v) = \frac{1}{2}\int_0^\xi \frac{d\xi(1-\varkappa^2\xi)}{\sqrt{\xi(1-\xi)(1-\varkappa^2\xi)}},$$

(8) $$E = \frac{1}{2}\int_0^1 \frac{d\xi(1-\varkappa^2\xi)}{\sqrt{\xi(1-\xi)(1-\varkappa^2\xi)}},$$

wo letzteres Integral in demselben Sinne zu nehmen ist, wie § 42 (17).

$E(v)$ und $Z(v)$ sind ungerade Funktionen des Arguments.

Aus dem Additionstheorem der Θ-Funktion [§ 43 (11)] ergibt sich durch logarithmische Differentiation:

$$(9)\qquad Z(u+v)+Z(u-v)=2Z(u)-\frac{2\varkappa^2\operatorname{sn}^2 v\operatorname{sn}u\operatorname{cn}u\operatorname{dn}u}{1-\varkappa^2\operatorname{sn}^2 u\operatorname{sn}^2 v},$$

$$(10)\qquad Z(u+v)-Z(u-v)=2Z(v)-\frac{2\varkappa^2\operatorname{sn}^2 u\operatorname{sn}v\operatorname{cn}v\operatorname{dn}v}{1-\varkappa^2\operatorname{sn}^2 u\operatorname{sn}^2 v}.$$

Hierin kann Z auch durch E ersetzt werden und durch Addition ergibt sich [§ 44 (16)]:

$$(11)\qquad E(u)+E(v)-E(u+v)=\varkappa^2\operatorname{sn}u\operatorname{sn}v\operatorname{sn}(u+v).$$

Hieraus erhält man die Periodeneigenschaften der Funktion $E(u)$, wenn man $v=\pm K,\ K+iK'$ setzt. Man kommt aber auch auf folgendem Wege dazu.

Aus der ersten Gleichung § 43 (3) folgt:

$$\frac{d\log H(v)}{dv}=Z(v+iK')+\frac{i\pi}{2K},$$

und demnach aus § 43 (6) und § 42 (11):

$$(12)\qquad \begin{aligned} Z(v+iK') &= Z(v)+\frac{\operatorname{cn}v\operatorname{dn}v}{\operatorname{sn}v}-\frac{i\pi}{2K},\\ Z(v+K) &= Z(v)-\frac{\varkappa^2\operatorname{sn}v\operatorname{cn}v}{\operatorname{dn}v}, \end{aligned}$$

und wenn man in der ersten dieser Formeln $v=K$ setzt:

$$(13)\qquad Z(K+iK')=-\frac{i\pi}{2K}.$$

Durch zweimalige Anwendung der Formeln (12) [mit Rücksicht auf § 44 (18), (20)]:

$$(14)\qquad \begin{aligned} Z(v+2iK') &= Z(v)-\frac{i\pi}{K},\\ Z(v+2K) &= Z(v). \end{aligned}$$

Überträgt man diese Gleichungen auf die Funktion $E(v)$, so folgt:

$$(15)\qquad \begin{aligned} E(v+iK') &= E(v)+\frac{\operatorname{cn}v\operatorname{dn}v}{\operatorname{sn}v}+\frac{iEK'}{K}-\frac{i\pi}{2K},\\ E(v+K) &= E(v)+E-\frac{\varkappa^2\operatorname{sn}v\operatorname{cn}v}{\operatorname{dn}v}. \end{aligned}$$

$$(16)\qquad \begin{aligned} E(v+2iK') &= E(v)+\frac{2iEK'}{K}-\frac{i\pi}{K},\\ E(v+2K) &= E(v)+2E. \end{aligned}$$

Wenn wir in (15) $v = K$ setzen und eine Größe E' durch die Gleichung definieren:

$$E(K + iK') = E + i(K' - E'), \tag{17}$$

so erhält man die unter dem Namen der Legendreschen Relation bekannte Formel

$$EK' + KE' - KK' = \frac{\pi}{2}. \tag{18}$$

Die Bedeutung der hier eingeführten Größe E' erkennt man, wenn man die Legendresche Relation auf einem zweiten Wege ableitet, mit Benutzung einer der linearen Transformationen.

Es ergibt sich, wenn man in § 31 (11) setzt:

$$u = \frac{v}{2K}, \qquad \omega = \frac{iK'}{K}, \qquad \frac{u}{\omega} = \frac{v}{2iK'},$$

nach § 43 (1), (4):

$$\sqrt{K}\, e^{-\frac{\pi v^2}{4KK'}}\, \Theta(iv, \varkappa') = \sqrt{K'}\, H(v + K), \tag{19}$$

und daraus durch logarithmische Differentiation

$$iZ(iv, \varkappa') = \frac{\pi v}{2KK'} + \frac{H'(v + K)}{H(v + K)} \tag{20}$$

oder nach § 43 (6)

$$iZ(iv, \varkappa') = \frac{\pi v}{2KK'} + Z(v) + \frac{d \log \operatorname{cn} v}{dv}. \tag{21}$$

Es ist aber nach (5)

$$i\frac{dZ(iv, \varkappa')}{dv} = -\operatorname{dn}^2(iv, \varkappa') + \frac{E'}{K'},$$

wenn jetzt E' die Bedeutung hat:

$$E' = \int_0^{K'} \operatorname{dn}^2(v, \varkappa')\, dv, \tag{22}$$

also aus E durch Vertauschung von $\varkappa$ mit $\varkappa'$ hervorgeht. Setzt man aber in (21) $v = 0$, nachdem man zuvor differentiiert hat, so ergibt sich wiederum die Relation (18), woraus folgt, daß E' beide Male dieselbe Größe ist.

§ 48. Die elliptischen Transzendenten dritter Gattung.

Wenn wir die Formel (10) des vorigen Paragraphen:

$$\frac{\Theta'(u + v)}{\Theta(u + v)} - \frac{\Theta'(u - v)}{\Theta(u - v)} = 2Z(v) - \frac{2\varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v}$$

in bezug auf u integrieren, so folgt:

$$(1) \qquad \frac{1}{2}\log\frac{\Theta(u-v)}{\Theta(u+v)} + u Z(v) = \int_0^u \frac{\varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1-\varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v} du,$$

und wir können noch die auf gleiche Weise [aus § 43 (11)] herzuleitende Formel:

$$(2) \qquad \frac{1}{2}\log\frac{H(v-u)}{H(v+u)} + u Z(v) = \int_0^u \frac{\operatorname{sn} v \operatorname{cn} v \operatorname{dn} v\, du}{\operatorname{sn}^2 u - \operatorname{sn}^2 v}$$

hinzufügen, die übrigens auch aus (1) abgeleitet werden kann. Wir setzen nun mit Jacobi

$$(3) \qquad \Pi(u, v) = \int_0^u \frac{\varkappa^2 \operatorname{sn}^2 u \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1-\varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v} du,$$

und nennen $\Pi(u, v)$ die Transzendente dritter Gattung mit dem Argument u und dem Parameter v. Ersetzt man du durch den Ausdruck:

$$\frac{d\xi}{2\sqrt{\xi(1-\xi)(1-\varkappa^2\xi)}}$$

und $\operatorname{sn}^2 u$ durch ξ, so ergibt sowohl (1) als (2) ein elliptisches Integral dritter Gattung, wie wir es in § 11 kennen gelernt haben.

Aus (1) folgt zunächst

$$(4) \qquad \Pi(u, v) - u Z(v) = \Pi(v, u) - v Z(u),$$

oder der Jacobische Satz über die Vertauschung von Argument und Parameter.

Die Funktion $\Pi(u, v)$ verschwindet, wenn $v = K$ oder $v = K + iK'$ ist, weil für den ersteren Wert $\operatorname{cn} v$, für den zweiten $\operatorname{dn} v$ gleich Null ist. Setzen wir daher diese Werte für u in (4) ein, so folgt

$$(5) \qquad \begin{aligned} \Pi(K, v) &= K Z(v) \\ \Pi(K+iK', v) &= (K+iK') Z(v) + \frac{i\pi v}{2K} \text{ [§ 47, (13)]}, \end{aligned}$$

wodurch die vollständigen Integrale dritter Gattung auf die zweite Gattung zurückgeführt sind.

Wir wollen noch das Additionstheorem der Π-Funktion ableiten, das Jacobi in den Fund. nova art. 53—55[1]) in ver-

[1]) C. G. J. Jacobis gesammelte Werke, Berlin 1881, Bd. I, S. 204.

schiedenen Formen gibt, die nur mühsam aufeinander zurückführbar sind. Zunächst erhalten wir aus der Definition (1), wenn wir den Parameter jetzt mit a bezeichnen:

$$\begin{aligned} &\Pi(u+v, a) - \Pi(u, a) - \Pi(v, a) \\ (6) \qquad &= \frac{1}{2}\log\frac{\Theta(u+v-a)}{\Theta(u+v+a)}\frac{\Theta(u+a)\,\Theta(v+a)}{\Theta(u-a)\,\Theta(v-a)}, \end{aligned}$$

und es handelt sich noch darum, den unter dem Logarithmus stehenden Ausdruck durch elliptische Funktionen darzustellen.

Dies geschieht zunächst leicht, wie an der erwähnten Stelle der Fundamenta, mittels der Formel [§ 43, (11)]:

$$\Theta^2(0)\,\Theta(u+v)\,\Theta(u-v) = \Theta^2(u)\,\Theta^2(v)\,[1 - \varkappa^2 \operatorname{sn}^2 u \operatorname{sn}^2 v],$$

wenn man darin für u, v setzt $u \pm a$, $v \pm a$, dann $\pm a$, $u + v \pm a$. Man erhält so:

$$\begin{aligned} &\Theta^2(0)\,\Theta(u+v\pm 2a)\,\Theta(u-v) \\ &= \Theta^2(u\pm a)\,\Theta^2(v\pm a)\,[1 - \varkappa^2 \operatorname{sn}^2(u\pm a)\operatorname{sn}^2(v\pm a)], \\ &\Theta^2(0)\,\Theta(u+v\pm 2a)\,\Theta(u+v) \\ &= \Theta^2(a)\,\Theta^2(u+v\pm a)\,[1 - \varkappa^2 \operatorname{sn}^2 a \operatorname{sn}^2(u+v\pm a)], \end{aligned}$$

woraus folgt:

$$\begin{aligned} (7) \qquad &\frac{\Theta(u+v-a)\,\Theta(u+a)\,\Theta(v+a)}{\Theta(u+v+a)\,\Theta(u-a)\,\Theta(v-a)} \\ &= \sqrt{\frac{[1-\varkappa^2\operatorname{sn}^2(u-a)\operatorname{sn}^2(v-a)]\,[1-\varkappa^2\operatorname{sn}^2 a \operatorname{sn}^2(u+v+a)]}{[1-\varkappa^2\operatorname{sn}^2(u+a)\operatorname{sn}^2(v+a)]\,[1-\varkappa^2\operatorname{sn}^2 a \operatorname{sn}^2(u+v-a)]}}. \end{aligned}$$

Einen zweiten Ausdruck erhält man aus der Additionsformel (13), § 22, die man so darstellen kann:

$$\begin{aligned} &\Theta(0)\,\Theta(u\pm a)\,\Theta(v\pm a)\,\Theta(u+v) \\ &= \Theta(u)\,\Theta(v)\,\Theta(a)\,\Theta(u+v\pm a)\,[1 \pm \varkappa^2 \operatorname{sn} a \operatorname{sn} u \operatorname{sn} v \operatorname{sn}(u+v\pm a)], \end{aligned}$$

woraus durch Division:

$$(8) \qquad \frac{\Theta(u+v-a)\,\Theta(u+a)\,\Theta(v+a)}{\Theta(u+v+a)\,\Theta(u-a)\,\Theta(v-a)} = \frac{1+\varkappa^2\operatorname{sn} a \operatorname{sn} u \operatorname{sn} v \operatorname{sn}(u+v+a)}{1-\varkappa^2\operatorname{sn} a \operatorname{sn} u \operatorname{sn} v \operatorname{sn}(u+v-a)}.$$

Jacobi gibt noch einen dritten Ausdruck für die Θ-Quotienten in (6):

$$(9) \qquad \frac{\left\{1-\varkappa^2\operatorname{sn}^2\left(\frac{u-v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}+a\right)\right\}\left\{1-\varkappa^2\operatorname{sn}^2\left(\frac{u+v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}-a\right)\right\}}{\left\{1-\varkappa^2\operatorname{sn}^2\left(\frac{u-v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}-a\right)\right\}\left\{1-\varkappa^2\operatorname{sn}^2\left(\frac{u+v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}+a\right)\right\}}.$$

Die direkte Überführung der drei Ausdrücke (7), (8), (9) ineinander gelingt am einfachsten, wenn man von der von **Jacobi** zuletzt gegebenen Formel ausgeht:

$$(10)\qquad \begin{aligned} &1 - \varkappa^2 \operatorname{sn}(a+u)\operatorname{sn}(a-u)\operatorname{sn}(a+v)\operatorname{sn}(a-v) \\ &= \frac{(1-\varkappa^2\operatorname{sn}^4 a)(1-\varkappa^2\operatorname{sn}^2 u\operatorname{sn}^2 v)}{(1-\varkappa^2\operatorname{sn}^2 a\operatorname{sn}^2 u)(1-\varkappa^2\operatorname{sn}^2 a\operatorname{sn}^2 v)}. \end{aligned}$$

Die Verifikation dieser Formel ist darum leicht, weil man mit Hilfe von § 44, (13) rechts und links rationale Funktionen von $\operatorname{sn}^2 u$, $\operatorname{sn}^2 v$ erhält, deren Identität unmittelbar ersichtlich ist.

Ersetzt man in dieser Formel

$$u,\qquad v,\qquad a$$

durch

$$\frac{u-v}{2},\qquad \frac{u+v}{2}\pm a,\qquad \frac{u+v}{2},$$

so ergibt sich

$$\begin{aligned} &1 \pm \varkappa^2 \operatorname{sn} u \operatorname{sn} v \operatorname{sn} a \operatorname{sn}(u+v\pm a) \\ &= \frac{\left[1-\varkappa^2\operatorname{sn}^4\left(\frac{u+v}{2}\right)\right]\left[1-\varkappa^2\operatorname{sn}^2\left(\frac{u-v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}\pm a\right)\right]}{\left[1-\varkappa^2\operatorname{sn}^2\left(\frac{u+v}{2}\right)\operatorname{sn}^2\frac{u-v}{2}\right]\left[1-\varkappa^2\operatorname{sn}^2\left(\frac{u+v}{2}\right)\operatorname{sn}^2\left(\frac{u+v}{2}\pm a\right)\right]}, \end{aligned}$$

und wenn man die beiden hierin enthaltenen Formeln durcheinander dividiert, so ergibt sich die Übereinstimmung von (8) und (9).

Setzt man in (10) $v = u$, so ergibt sich:

$$(11)\qquad 1-\varkappa^2\operatorname{sn}^2(a+u)\operatorname{sn}^2(a-u) = \frac{(1-\varkappa^2\operatorname{sn}^4 a)(1-\varkappa^2\operatorname{sn}^4 u)}{(1-\varkappa^2\operatorname{sn}^2 a\operatorname{sn}^2 u)^2}.$$

Ersetzt man hierin

$$a\qquad u$$

zuerst durch

$$\frac{u+v}{2}\pm a,\qquad -\frac{u+v}{2},$$

sodann durch

$$\frac{u+v}{2}\pm a,\qquad \frac{u-v}{2},$$

so ergeben sich vier Formeln:

$$\begin{aligned} &1-\varkappa^2\operatorname{sn}^2 a\operatorname{sn}^2(u+v\pm a) \\ &= \frac{\left[1-\varkappa^2\operatorname{sn}^4\left(\frac{u+v}{2}\pm a\right)\right]\left(1-\varkappa^2\operatorname{sn}^4\frac{u+v}{2}\right)}{\left[1-\varkappa^2\operatorname{sn}^2\left(\frac{u+v}{2}\pm a\right)\operatorname{sn}^2\frac{u+v}{2}\right]^2}, \end{aligned}$$

$$1 - \varkappa^2 \operatorname{sn}^2(u \pm a)\operatorname{sn}^2(v \pm a)$$

$$= \frac{\left[1 - \varkappa^2 \operatorname{sn}^4\left(\frac{u+v}{2} \pm a\right)\right]\left(1 - \varkappa^2 \operatorname{sn}^4 \frac{u-v}{2}\right)}{\left[1 - \varkappa^2 \operatorname{sn}^2\left(\frac{u+v}{2} \pm a\right)\operatorname{sn}^2\left(\frac{u-v}{2}\right)\right]^2},$$

woraus sich die Übereinstimmung von (9) mit (7) ergibt.

§ 49. Die Transzendenten zweiter und dritter Gattung von Weierstrass.

Es sind nun noch die Transzendenten zweiter und dritter Gattung in der Weierstrassschen Form aufzustellen. Zu der ersteren gelangen wir ähnlich wie in § 47 durch zweimalige Differentiation von $\log \sigma(u)$. Es ergibt sich so aus

$$(1) \qquad \sigma(u) = \omega_1 e^{\frac{\eta_1 u^2}{\omega_1}} \frac{\vartheta_{11}\left(\frac{u}{\omega_1}\right)}{\vartheta'_{11}} \quad [\S\ 37,\ (4)],$$

$$\frac{d^2 \log \sigma(u)}{du^2} = \frac{2\eta_1}{\omega_1} + \frac{d^2 \log \vartheta_{11}\left(\frac{u}{\omega_1}\right)}{du^2},$$

$$= \frac{2\eta_1}{\omega_1} + \frac{1}{\omega_1^2}\frac{\vartheta''_{00}}{\vartheta_{00}} - \frac{1}{\omega_1^2}\frac{\vartheta'^2_{11}}{\vartheta^2_{00}} \frac{\vartheta^2_{00}\left(\frac{u}{\omega_1}\right)}{\vartheta^2_{11}\left(\frac{u}{\omega_1}\right)} \quad [\S\ 23,\ (18)]$$

und also, wenn man den ϑ-Quotienten nach § 42 durch elliptische Funktionen und diese nach § 46 durch die $\wp$-Funktion ausdrückt:

$$\frac{d^2 \log \sigma(u)}{du^2} = A - \wp(u),$$

worin A eine Konstante ist. Diese findet man aber, wenn man die Gleichung nach § 46, (8) so schreibt:

$$\sigma''(u)\sigma(u) - \sigma'(u)\sigma'(u) = A\sigma^2(u) - \tfrac{1}{3}[\sigma^2_{00}(u) + \sigma^2_{01}(u) + \sigma^2_{10}(u)].$$

Wenn man hierin zweimal differentiiert und dann $u = 0$ setzt, so ergibt sich $A = 0$ [§ 35, (12), § 37, (5), (7)], und wir erhalten:

$$(2) \qquad \frac{d^2 \log \sigma(u)}{du^2} = -\wp(u),$$

eine Formel, die bei Weierstrass zur Definition der $\wp$-Funktion dient.

Wird also

$$\frac{\sigma'(u)}{\sigma(u)} = \zeta(u) \tag{3}$$

gesetzt, so ist $\zeta(u)$ eine eindeutige Funktion von u, und zwar ein elliptisches Integral zweiter Gattung:

$$\zeta(u) = -\int \wp(u)\,du = -\int \frac{\wp\, d\wp}{\sqrt{4\wp^3 - g_2\wp - g_3}} \quad [\S\ 46,\ (19)], \tag{4}$$

worin die additive Konstante dadurch bestimmt ist, daß $\zeta(u)$ eine ungerade Funktion sein muß. Die Periodizität der ζ-Funktion ergibt sich aus den Periodengleichungen der σ-Funktion [§ 35, (9)]:

$$\begin{aligned} \zeta(u + \omega_1) - \zeta(u) &= 2\eta_1, \\ \zeta(u + \omega_2) - \zeta(u) &= 2\eta_2. \end{aligned} \tag{5}$$

Es sind also $2\eta_1$ und $2\eta_2$ als vollständige Integrale zweiter Gattung (analog den E, E') dargestellt:

$$2\eta_1 = -\int_u^{u+\omega_1} \wp(u)\,du, \quad 2\eta_2 = -\int_u^{u+\omega_2} \wp(u)\,du \tag{6}$$

mit der der Legendreschen Relation entsprechenden Gleichung

$$\eta_1\omega_2 - \eta_2\omega_1 = \pi i \quad [\S\ 35,\ (10)]. \tag{7}$$

Um die Additionstheoreme für die Weierstrassschen Transzendenten zu bilden, gehen wir von der σ-Funktion aus. Für diese erhalten wir aus (1) mit Benutzung der Additionsformel für ϑ_{11}, § 22, (4):

$$\frac{\sigma(u+v)\,\sigma(u-v)}{\sigma(u)^2\,\sigma(v)^2} = \wp(v) - \wp(u), \tag{8}$$

daraus durch logarithmische Differentiation:

$$\begin{aligned} \zeta(u+v) + \zeta(u-v) - 2\zeta(u) &= \frac{\wp'(u)}{\wp(u) - \wp(v)}, \\ \zeta(u+v) - \zeta(u-v) - 2\zeta(v) &= \frac{-\wp'(v)}{\wp(u) - \wp(v)}, \end{aligned} \tag{9}$$

$$\zeta(u+v) = \zeta(u) + \zeta(v) + \frac{1}{2}\,\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}. \tag{10}$$

Hieraus leitet man durch abermalige Differentiation das Additionstheorem für die $\wp$-Funktion her. Man erhält aus (9) durch Differentiation nach u und v:

$$\wp(u+v)+\wp(u-v)-2\wp(u)=-\frac{\wp''(u)}{\wp(u)-\wp(v)}+\frac{\wp'(u)^2}{[\wp(u)-\wp(v)]^2},$$

$$2\wp(u+v)-2\wp(u-v)=-\frac{2\wp'(u)\wp'(v)}{[\wp(u)-\wp(v)]^2},$$

$$\wp(u+v)+\wp(u-v)-2\wp(v)=\frac{\wp''(v)}{\wp(u)-\wp(v)}+\frac{\wp'(v)^2}{[\wp(u)-\wp(v)]^2},$$

und indem man addiert:

$$4\wp(u+v)-2\wp(u)-2\wp(v)=\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2-\frac{\wp''(u)-\wp''(v)}{\wp(u)-\wp(v)}.$$

Es ist aber

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u) - g_3,$$
$$\wp''(u) = 6\wp(u)^2 - \tfrac{1}{2}g_2,$$
$$\wp''(u) - \wp''(v) = 6[\wp^2(u) - \wp^2(v)],$$

woraus man erhält:

$$(11) \qquad \wp(u+v)+\wp(u)+\wp(v)=\frac{1}{4}\left(\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}\right)^2,$$

in Übereinstimmung mit der Formel (21), § 13.

Endlich erhält man noch durch Integration der zweiten Gleichung (9) in bezug auf u:

$$(12) \qquad \frac{1}{2}\log\frac{\sigma(v-u)}{\sigma(v+u)}+u\zeta(v)=\frac{1}{2}\int_0^u\frac{\wp'(v)\,du}{\wp(u)-\wp(v)},$$

wodurch ein Integral dritter Gattung vom Argument u und dem Parameter v durch die σ-Funktion ausgedrückt ist.

Eine andere Form des Integrals dritter Gattung erhält man durch Integration von (10):

$$(13) \qquad \log\frac{\sigma(u+v)}{\sigma(u)\sigma(v)}-u\zeta(v)=\frac{1}{2}\int\frac{\wp'(u)-\wp'(v)}{\wp(u)-\wp(v)}du.$$

§ 50. Entwickelungen der elliptischen Funktionen.

Setzt man in den Entwickelungen der Theta-Quotienten, die in § 26 abgeleitet und in der Tabelle II zusammengestellt sind, $a=0$, so erhält man, wenn man zunächst die Formeln, die $\vartheta_{11}(a)$ im Nenner enthalten, wegläßt, die Partialbruchentwickelungen von zwölf elliptischen Funktionen:

$$\begin{array}{lll} \operatorname{sn} 2Ku, & \operatorname{cn} 2Ku, & \operatorname{dn} 2Ku, \\ \frac{1}{\operatorname{sn} 2Ku}, & \frac{\operatorname{cn} 2Ku}{\operatorname{sn} 2Ku}, & \frac{\operatorname{dn} 2Ku}{\operatorname{sn} 2Ku}, \\ \frac{1}{\operatorname{cn} 2Ku}, & \frac{\operatorname{sn} 2Ku}{\operatorname{cn} 2Ku}, & \frac{\operatorname{dn} 2Ku}{\operatorname{cn} 2Ku}, \\ \frac{1}{\operatorname{dn} 2Ku}, & \frac{\operatorname{sn} 2Ku}{\operatorname{dn} 2Ku}, & \frac{\operatorname{cn} 2Ku}{\operatorname{dn} 2Ku}. \end{array}$$

So ergibt sich aus der Formel (2), Tabelle II:

$$\frac{\vartheta'_{11}\vartheta_{10}(u)}{\pi\vartheta_{11}(u)\vartheta_{10}} = \operatorname{cotg}\pi u - 2i\Sigma(-1)^{\frac{m}{2}} q^m\left(\frac{1}{e^{-2\pi i u} - q^m} - \frac{1}{e^{2\pi i u} - q^m}\right)$$

$$= \operatorname{cotg}\pi u + 4\sin 2\pi u \sum \frac{(-1)^{\frac{m}{2}} q^m}{1 - 2q^m\cos 2\pi u + q^{2m}},$$

worin m die Reihe der positiven geraden Zahlen 2, 4, 6, 8, ... durchläuft.

Es ist aber nach § 42, (4)

$$\frac{\vartheta_{10}(u)}{\vartheta_{11}(u)} = \frac{\vartheta_{00}}{\vartheta_{01}} \frac{\operatorname{cn} 2Ku}{\operatorname{sn} 2Ku},$$

und daraus ergibt sich

$$(1) \quad \frac{2K}{\pi}\frac{\operatorname{cn} 2Ku}{\operatorname{sn} 2Ku} = \operatorname{cotg}\pi u + 4\sin 2\pi u \sum \frac{(-1)^{\frac{m}{2}} q^m}{1 - 2q^m\cos \pi u + q^{2m}}.$$

Wenn man in der Formel (2) der Tabelle III das gleiche Verfahren anwendet, so erhält man:

$$\frac{2K}{\pi}\frac{\operatorname{cn} 2Ku}{\operatorname{sn} 2Ku} = \operatorname{cotg}\pi u + 4\sum(-1)^{\frac{m'}{2}} q^{\frac{mm'}{2}} \sin\pi m u.$$

Hierin durchlaufen m und m' voneinander unabhängig die Reihen der positiven geraden Zahlen, und es läßt sich die Summation in bezug auf m' noch ausführen:

$$\sum(-1)^{\frac{m'}{2}} q^{\frac{mm'}{2}} = -\frac{q^m}{1+q^m},$$

also:

$$(2) \quad \frac{2K}{\pi}\frac{\operatorname{cn} 2Ku}{\operatorname{sn} 2Ku} = \operatorname{cotg}\pi u - 4\sum\frac{q^m}{1+q^m}\sin\pi m u.$$

Während aber die beiden ersten Formeln für alle Werte von u konvergieren, ist die Konvergenz der dritten auf das Gebiet beschränkt, in dem der imaginäre Teil von u absolut kleiner ist als der imaginäre Teil von ω. Die Formel ist also für reelle u jedenfalls gültig.

In der Tabelle IV sind die Entwickelungen für die 12 Funktionen zusammengestellt.

Unter den 16 Formeln der Tabellen II, III finden sich vier, die den Faktor $\vartheta_{11}(a)$ im Nenner enthalten, in denen man also nicht ohne weiteres $a = 0$ setzen kann. Es sind dies die Formeln (1), (5), (9), (13). Entwickelt man in diesen Formeln nach steigenden Potenzen von a, so fangen die Entwickelungen rechts und links mit a^{-1} an, und wenn man die von a unabhängigen Glieder beiderseits einander gleich setzt, so ergeben sich die gesuchten Entwickelungen.

Man kann etwa so verfahren, daß man in der Formel (1) a in $-a$ verwandelt und das arithmetrische Mittel aus beiden Formeln nimmt. Dann hebt sich rechts das unendliche Glied $1 : \operatorname{cotg} \pi a$ heraus und links erhält man:

$$\frac{\vartheta'_{11}[\vartheta_{11}(v+a) - \vartheta_{11}(v-a)]}{2\pi\vartheta_{11}(v)\vartheta_{11}(a)} = \frac{\vartheta'_{11}(v)}{\pi\vartheta_{11}(v)} \text{ für } a = 0,$$

auf der rechten Seite von (1) in Tabelle II ergibt sich:

$$\operatorname{cotg} \pi v - 4i\sum\left(\frac{q^m}{e^{-2\pi i v} - q^m} - \frac{q^m}{e^{2\pi i v} - q^m}\right)$$

$$= \operatorname{cotg} \pi v + 4\sum \frac{q^m \sin 2\pi v}{1 - 2q^m \cos 2\pi v + q^{2m}},$$

und auf der rechten Seite der Formel (1) der Tabelle III erhält man

$$\operatorname{cotg} \pi v + 4\sum \frac{q^{\frac{m}{2}}}{1 - q^m} \sin m\pi v,$$

und wenn man noch die Jacobische H-Funktion einführt, und u für v schreibt, erhält man

$$(3)\quad \frac{2K}{\pi}\frac{d\log H(2Ku)}{d\,2Ku} = \operatorname{cotg}\pi u + 4\sin 2\pi u \sum \frac{q^m}{1 - 2q^m\cos 2\pi u + q^m}$$

$$= \operatorname{cotg} \pi u + 4\sum \frac{q^m}{1 - q^m} \sin m\pi u.$$

Auf der linken Seite steht eine Transzendente zweiter Gattung, die sich nach § 47, (12) durch die Z-Funktion ausdrücken läßt:

$$\frac{2K}{\pi} Z(2Ku) + \frac{2K}{\pi}\frac{\operatorname{cn} 2Ku \operatorname{dn} 2Ku}{\sin 2Ku},$$

wofür man auch setzen kann:

$$\frac{2K}{\pi} Z(2Ku) + \frac{d\log\sin 2Ku}{\pi\, du}.$$

In der Tabelle V sind die vier Formeln, die sich auf diese Weise ergeben, zusammengestellt. Subtrahiert man die Formel (3) dieser Tabelle von den drei übrigen, so ergeben sich Entwickelungen für die logarithmischen Ableitungen der drei elliptischen Grundfunktionen, von denen wir die eine anführen wollen:

$$(4)\quad \frac{d\log \operatorname{sn} 2Ku}{\pi\, du} = \frac{d\log\sin\pi u}{\pi\, du} + 4\sin 2\pi u \sum_{h=1}^{\infty} \frac{(-1)^h q^h}{1-2q^h\cos 2\pi u + q^{2h}}$$

$$= \frac{d\log\sin\pi u}{\pi\, du} - 4\sum_{h=1}^{\infty} \frac{q^h \sin 2h\pi u}{1+q^h}.$$

Entwickelungen für die Transzendenten **dritter Gattung** ergeben sich, wenn man die Formeln der fünften Tabelle zwischen den Grenzen $u+v$, $u-v$ integriert. Man erhält so z. B. aus der Formel (3) dieser Tabelle:

$$(5)\quad \frac{1}{2}\log\frac{\theta[2K(u-v)]}{\theta[2K(u+v)]} = -4\sum \frac{q^{\frac{m}{2}}}{m(1-q^m)} \sin m\pi u \sin m\pi v.$$

Setzt man in den Formeln der Tabelle IV und V $u=0$, so ergeben sich die folgenden Entwickelungen:

$$\frac{2K}{\pi} = 1 + 4\sum \frac{q^{\frac{m}{2}}}{1+q^m} = 1 + 4\sum \frac{(-1)^{\frac{n-1}{2}} q^n}{1-q^n},$$

$$\frac{2\varkappa K}{\pi} = 4\sum \frac{q^{\frac{n}{2}}}{1+q^n} = 4\sum \frac{(-1)^{\frac{n-1}{2}} q^{\frac{n}{2}}}{1-q^n},$$

$$\frac{2\varkappa' K}{\pi} = 1 + 4\sum \frac{(-1)^{\frac{m}{2}} q^{\frac{m}{2}}}{1+q^m} = 1 - 4\sum \frac{(-1)^{\frac{n-1}{2}} q^n}{1+q^n}.$$

Endlich erhält man eine Entwickelung für das vollständige Integral zweiter Gattung E aus der Formel

$$Z(v) = E(v) - \frac{E}{K} v.$$

Setzt man hierin nach der Differentiation $v=0$, so folgt:

$$Z'(0) = \frac{K-E}{K},$$

und mithin nach der Tabelle V, Formel (3):

$$K - E = \frac{2\pi^2}{K}\sum \frac{q^n}{(1-q^n)^2} = \frac{\pi^2}{K}\sum \frac{m q^{\frac{m}{2}}}{1-q^m}.$$

Fünfter Abschnitt.

Die Modulfunktionen.

§ 51. Die elliptischen Differentialgleichungen.

Die bisher definierten elliptischen Funktionen sind Funktionen der beiden Variablen v, ω, und die Moduln $\varkappa$, $\varkappa'$, ferner $j(\omega)$, K, K' sind von dem Periodenverhältnis ω, das einen positiv imaginären Bestandteil haben muß, abhängig. Ebenso ist die Funktion $\wp(u)$ eine Funktion der drei Variablen u, ω_1, ω_2 und die Invarianten g_2, g_3 sind von ω_1, ω_2 abhängig. Die Aufgabe der Umkehrung der elliptischen Integrale, wie wir sie in § 14 formuliert haben, setzt aber voraus, daß in den elliptischen Funktionen $\varkappa^2$ (oder bei der Weierstrassschen Normalform g_2, g_3) beliebig gegebene Werte haben, und die vollständige Lösung dieser Aufgabe verlangt also, daß nicht ω, sondern $\varkappa^2$ (bzw. g_2, g_3) als zweite unabhängige Variable auftritt, und daß ω durch diese ausgedrückt werde. Dieser Aufgabe werden die nächsten Betrachtungen gewidmet sein.

Wir gehen aus von der Aufgabe, ein System von Differentialgleichungen, welches wir das der elliptischen Differentialgleichungen nennen, zu integrieren:

$$\frac{dx}{dv} = yz, \qquad \frac{dy}{dv} = -zx, \qquad \frac{dz}{dv} = -\varkappa^2 xy, \tag{1}$$

unter den Nebenbedingungen:

(2) für $v = 0$ soll $x = 0$, $y = 1$, $z = 1$ sein.

Wir haben im vorigen Abschnitt gesehen, daß, wenn

$$(3) \qquad \varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4}$$

ist, diese Aufgabe durch die elliptischen Funktionen gelöst wird, und zwar in der Weise, daß x, y, z in der ganzen v-Ebene eindeutige und, außer wo sie unendlich sind, stetige Funktionen von v werden. Ist nun aber $\varkappa^2$ gegeben, so entsteht die Frage, ob es zu jedem Wert von $\varkappa^2$ einen der Bedingung (3) genügenden Wert von ω gibt und ob es mehrere solche gibt.

Wir beweisen zunächst, daß durch die Differentialgleichungen (1) mit den Nebenbedingungen die Funktionen x, y, z eindeutig bestimmt sind.

Es ergibt sich zunächst aus (1), daß $x^2 + y^2$, $\varkappa^2 x^2 + z^2$ konstant sind, und aus den Nebenbedingungen folgt:

$$(4) \qquad y^2 = 1 - x^2, \qquad z^2 = 1 - \varkappa^2 x^2.$$

Angenommen, es existiere ein zweites System denselben Bedingungen genügender Funktionen x_1, y_1, z_1, so ist zunächst

$$y_1^2 = 1 - x_1^2, \qquad z_1^2 = 1 - \varkappa^2 x_1^2,$$

und eine einfache Differentiation ergibt, daß

$$\frac{x y_1 z_1 - x_1 y z}{1 - \varkappa^2 x^2 x_1^2}$$

konstant ist. (Das Additionstheorem der elliptischen Integrale, aus dem man die Form dieses Ausdruckes erhält, wird unmittelbar durch Differentiation bestätigt.) Aus den Nebenbedingungen folgt aber, daß diese Konstante verschwindet, also:

$$x y_1 z_1 = x_1 y z,$$

woraus man leicht schließt, indem man beiderseits quadriert:

$$x = x_1, \qquad y = y_1, \qquad z = z_1.$$

§ 52. Die unabhängige Variable $\varkappa^2$. Lineare Differentialgleichung für K.

Wir zeigen nun zunächst, daß und wie man zu einem beliebig gegebenen Wert von $\varkappa^2$ wenigstens einen der Bedingung

$$(1) \qquad \varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4}$$

genügenden Wert von ω finden kann. Diese Frage wird am vollständigsten beantwortet durch Zurückführung auf eine lineare Differentialgleichung zweiter Ordnung.

Eine solche Differentialgleichung ist aber in den Formeln des § 23 bereits enthalten.

Es folgt zunächst aus § 23, (14):

$$d \log \varkappa^2 = i \pi \vartheta_{01}^4 \, d\omega,$$

oder mit Rücksicht auf

(2) $\pi \vartheta_{00}^2 = 2K, \quad \pi \vartheta_{10}^2 = 2\varkappa K, \quad \pi \vartheta_{01}^2 = 2\varkappa' K$ [§ 42, (3), (15)]:

(3) $$\pi \, d(\varkappa^2) = 4 i \varkappa^2 \varkappa'^2 K^2 \, d\omega,$$

und aus § 23, (19):

$$\frac{d}{d\omega} \frac{dK}{K^2 d\omega} = -\frac{4}{\pi^2} \varkappa^2 \varkappa'^2 K^3.$$

Führt man vermittelst (3) für ω die Variable $\varkappa^2$ ein, so folgt

(4) $$\frac{d}{d(\varkappa^2)} \left(\varkappa^2 \varkappa'^2 \frac{dK}{d(\varkappa^2)} \right) = \frac{1}{4} K,$$

und dies ist die gesuchte Differentialgleichung.

Setzen wir weiter

(5) $$-i\omega = \frac{K'}{K},$$

(6) $$-iK^2 d\omega = K dK' - K' dK,$$

so ergibt sich nach (3):

(7) $$\varkappa^2 \varkappa'^2 \left(K \frac{dK'}{d(\varkappa^2)} - K' \frac{dK}{d(\varkappa^2)} \right) = -\frac{\pi}{4},$$

also durch abermalige Differentiation:

$$\frac{1}{K} \frac{d}{d(\varkappa^2)} \left(\varkappa^2 \varkappa'^2 \frac{dK}{d(\varkappa^2)} \right) = \frac{1}{K'} \frac{d}{d(\varkappa^2)} \left(\varkappa^2 \varkappa'^2 \frac{dK'}{d(\varkappa^2)} \right),$$

woraus zu ersehen, daß K' das zweite partikulare Integral der Differentialgleichung (4) ist.

Diese Differentialgleichung läßt sich durch hypergeometrische Reihen integrieren (Gauss, Disq. circa seriem infinitum Werke, Bd. III, S. 125).

Setzen wir für den Augenblick $\varkappa^2 = x$, $K = y$, so lautet die Differentialgleichung (4)

(8) $$x(1-x) \frac{d^2 y}{dx^2} + (1 - 2x) \frac{dy}{dx} - \frac{1}{4} y = 0,$$

und sie geht aus der allgemeinen Gaussschen Differentialgleichung

(9) $$(x - x^2) \frac{d^2 y}{dx^2} + [\gamma - (\alpha + \beta + 1) x] \frac{dy}{dx} - \alpha \beta y = 0$$

hervor, wenn man $\alpha = \beta = \frac{1}{2}$, $\gamma = 1$ setzt. Das eine ihrer partikularen Integrale ist also

$$(10) \qquad F(\tfrac{1}{2}, \tfrac{1}{2}, 1, x) = 1 + \sum_{\nu=1}^{\infty} \left(\frac{1.3.5\ldots 2\nu - 1}{2.4\ldots 2\nu}\right)^2 x^\nu$$
$$= \sum_{\nu=0}^{\infty} \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{x}{16}\right)^\nu,$$

und diese Reihe ist konvergent, so lange der absolute Wert von x kleiner als 1 ist. Als das zweite partikulare Integral kann man wählen

$$(11) \qquad F(\tfrac{1}{2}, \tfrac{1}{2}, 1, 1 - x),$$

das aber einen anderen Konvergenzbereich hat. Denken wir uns x als komplexe Variable in einer Ebene dargestellt, so konvergiert (10) in einem mit dem Radius 1 um den Nullpunkt beschriebenen Kreise, (11) in einem gleichen Kreise um den Punkt 1 beschrieben, so daß der gemeinsame Konvergenzbereich aus einem Zweieck besteht, das den zwischen 0 und 1 gelegenen Teil der reellen Achse enthält. Man kann aber auch, was für uns wichtig ist, das zweite partikulare Integral in einer Form aufstellen, die in demselben Kreise wie die Reihe (10) konvergiert. Dabei ist zu beachten, daß das zweite partikulare Integral für $x = 0$ unendlich wird.

Dieses zweite partikulare Integral erhält man durch den folgenden Grenzübergang: Bezeichnen wir die hypergeometrische Reihe nach Gauss mit

$$F(\alpha, \beta, \gamma, x) = 1 + \frac{\alpha . \beta}{1 . \gamma} x + \frac{\alpha(\alpha + 1)\beta(\beta + 1)}{1.2.\gamma(\gamma + 1)} x^2 + \cdots$$
$$= \frac{\Pi(\gamma - 1)}{\Pi(\alpha - 1)\Pi(\beta - 1)} \sum_{\nu=0}^{\infty} \frac{\Pi(\alpha + \nu - 1)\Pi(\beta + \nu - 1)}{\Pi(\gamma + \nu - 1)\Pi(\nu)} x^\nu,$$

so erhält man im allgemeinen die beiden partikularen Integrale von (9):

$$y_1 = F_1(x) = F(\alpha, \beta, \gamma, x),$$
$$y_2 = F_2(x) = x^{1-\gamma}(1 - x)^{\gamma - \alpha - \beta} F(1 - \alpha, 1 - \beta, 2 - \gamma, x).$$

Da diese aber für $\alpha = \beta = \frac{1}{2}$, $\gamma = 1$ miteinander identisch werden, so setze man zunächst $\alpha = \beta = \frac{1}{2}$, $\gamma = 1 + \varepsilon$, also

$$y_1 = F(\tfrac{1}{2}, \tfrac{1}{2}, 1 + \varepsilon, x),$$
$$y_2 = \left(\frac{1 - x}{x}\right)^\varepsilon F(\tfrac{1}{2}, \tfrac{1}{2}, 1 - \varepsilon, x).$$

Es ist aber

$$F(\tfrac{1}{2}, \tfrac{1}{2}, 1 \pm \varepsilon, x) = \frac{\Pi(\pm\varepsilon)}{[\Pi(-\tfrac{1}{2})]^2} \sum_{\nu=0}^{\infty} \frac{\Pi(\nu-\tfrac{1}{2})^2}{\Pi(\nu\pm\varepsilon)\,\Pi(\nu)} x^\nu,$$

und man kann unter Hinzufügung eines konstanten Faktors als zweites partikulares Integral auch folgendes annehmen:

$$\frac{1}{2\varepsilon} \cdot \sum_{\nu=0}^{\infty} \frac{\Pi(\nu-\tfrac{1}{2})^2}{\Pi(\nu)} \left[\frac{-1}{\Pi(\nu+\varepsilon)} + \left(\frac{x}{1-x}\right)^{-\varepsilon} \frac{1}{\Pi(\nu-\varepsilon)}\right] x^\nu.$$

Entwickelt man hier nach Potenzen von ε und setzt dann $\varepsilon = 0$, so folgt:

$$\sum_{\nu=0}^{\infty} \frac{\Pi(\nu-\tfrac{1}{2})^2}{\Pi(\nu)^2} x^\nu \left[\frac{\Pi'(\nu)}{\Pi(\nu)} - \frac{1}{2}\log\frac{x}{1-x}\right],$$

wofür man mit Benutzung der Gaussschen Formel

$$\frac{\Pi(\nu-\tfrac{1}{2})\,\Pi(\nu)}{\Pi(2\nu)} = \sqrt{\pi}\,2^{-2\nu}$$

mit Abwerfung eines konstanten Faktors auch setzen kann:

$$(12) \qquad \sum_{\nu=0}^{\infty} \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{x}{16}\right)^\nu \left[\frac{\Pi'(\nu)}{\Pi(\nu)} - \frac{1}{2}\log\frac{x}{1-x}\right].$$

Es ist aber für ein ganzzahliges positives ν:

$$\frac{\Pi'(\nu)}{\Pi(\nu)} = \Pi'(0) + 1 + \tfrac{1}{2} + \tfrac{1}{3} + \cdots + \frac{1}{\nu},$$

und wenn wir also zur Abkürzung setzen:

$$(13) \qquad \begin{aligned} F(x) &= \sum_{\nu=0}^{\infty} \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(\frac{x}{16}\right)^\nu, \\ G(x) &= 2\sum_{\nu=1}^{\infty} \frac{\Pi(2\nu)^2}{\Pi(\nu)^4} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots \frac{1}{\nu}\right)\left(\frac{x}{16}\right)^\nu, \end{aligned}$$

so ergeben sich die beiden partikulären Lösungen der Differentialgleichung (8), wenn man für das zweite eine lineare Kombination von (10) und (12) nimmt:

$$(14) \qquad y_1 = F(x), \quad y_2 = \frac{1}{2} G(x) - \frac{1}{2}\log\frac{x}{16(1-x)} F(x).$$

Um nun aber die partikularen Integrale K und K' durch diese Funktionen darzustellen, müssen wir das Verhalten von K, K' für $q = 0$ untersuchen, wofür zugleich $\varkappa^2 = 0$ wird.

Es ist aber für $q = 0$ nach § 25 und § 42:

$$q^{-1}\varkappa^2 = 16, \qquad 2K = \pi,$$

also:
$$\text{Lim}\left(\log\frac{\varkappa^2}{16}-i\pi\omega\right)=0,$$
andererseits ist $2iK'=\pi\vartheta_{00}^2\omega$ (§ 42) oder:
$$2K'+\log\frac{\varkappa^2}{16}=\left(\log\frac{\varkappa^2}{16}-i\pi\omega\right)+i\pi\omega(1-\vartheta_{00}^2),$$
woraus:
$$\text{(15)}\qquad \lim_{\varkappa^2=0}\left(K'+\frac{1}{2}\log\frac{\varkappa^2}{16}\right)=0.$$

Da nun K und K' partikulare Integrale von (8) sind (für $x=\varkappa^2$), so haben beide die Form:
$$K=a_1y_1+a_2y_2,\qquad K'=a_1'y_1+a_2'y_2,$$
worin a_1, a_2, a_1', a_2' konstant sind. Da K für $x=0$ endlich bleibt und den Wert $\frac{1}{2}\pi$ erhält, so ist $a_2=0$, $a_1=\frac{1}{2}\pi$, und damit $K'+\frac{1}{2}\log x$ endlich bleibe und [nach (15)] den Wert $\log 4$ erhalte, muß $a_2'=1$ und $a_1'=0$ sein. Also ergibt sich, wenn man $x=\varkappa^2$, $1-x=\varkappa'^2$ setzt:
$$\text{(16)}\qquad K=\frac{\pi}{2}F(\varkappa^2),\quad K'=\frac{1}{2}G(\varkappa^2)-\frac{1}{2}\log\frac{\varkappa^2}{16\varkappa'^2}F(\varkappa^2)$$
und
$$\text{(17)}\qquad q=e^{-\frac{\pi K'}{K}}=\frac{\varkappa^2}{16\varkappa'^2}e^{-\frac{G(\varkappa^2)}{F(\varkappa^2)}},$$
worin, wie schon bemerkt, die Reihen $G(\varkappa^2)$, $F(\varkappa^2)$ konvergent sind, so lange der absolute Wert von $\varkappa^2$ ein echter Bruch ist. In der Differentialgleichung (4) liegen nun freilich die Mittel, die gefundenen Ausdrücke für K, K', q über dies Konvergenzbereich hinaus fortzusetzen. Einfacher gelangt man dazu aber durch die Anwendung der Landenschen Transformation.

Wir begrenzen die Ebene der komplexen Werte $\varkappa^2$, indem wir längs der reellen Achse zwei Schnitte von 0 bis $-\infty$ und von 1 bis ∞ legen. In der so begrenzten Ebene sind dann alle Wurzeln aus $\varkappa^2$, $\varkappa'^2$ eindeutig dadurch bestimmt, daß sie für positive echt gebrochene $\varkappa^2$ reell und positiv sein sollen. Es ist nun nach den Formeln der Landenschen Transformation [§ 44, (28)], wenn wir mit $\varkappa_1$, $\varkappa_1'$, K_1, K_1' die Funktionen von ω bezeichnen, die sich aus $\varkappa$, $\varkappa'$, K, K' ergeben, wenn ω durch 2ω ersetzt wird:
$$\text{(18)}\qquad \begin{gathered}\varkappa_1=\frac{1-\varkappa'}{1+\varkappa'},\qquad \varkappa_1'=\frac{2\sqrt{\varkappa'}}{1+\varkappa'},\\ 2K_1=(1+\varkappa')K,\quad K_1'=(1+\varkappa')K'.\end{gathered}$$

Wenn wir also in (17) ω durch 2ω ersetzen und die Quadratwurzel ziehen, so folgt:

$$(19)\qquad q = \frac{1}{4}\frac{\varkappa_1}{\varkappa_1'} e^{-\frac{1}{2}\frac{G(\varkappa_1^2)}{F(\varkappa_1^2)}}.$$

Hierin erstreckt sich nun der Konvergenzbereich über den in der Ebene $\varkappa_1^2$ gelegenen Einheitskreis und dieser entspricht der ganzen Ebene $\varkappa^2$. Denn der reelle Teil vom $\varkappa'$ ist in der ganzen Ebene der $\varkappa^2$ positiv mit Ausnahme der beiden Ufer des von $+1$ nach $+\infty$ verlaufenden Schnittes, an denen $\varkappa'$ rein imaginär ist. Daraus ergibt sich, daß der absolute Wert von $\varkappa_1$ kleiner als 1 ist, und daß die Peripherie des Einheitskreises in der Ebene $\varkappa_1$ den beiden Ufern dieses Schnittes entspricht.

Man kann aber die Konvergenz dieser Ausdrücke noch verbessern durch eine abermalige Anwendung der Landenschen Transformation. Bezeichnen wir das Resultat einer nochmaligen Verdoppelung von ω durch den Index 2, so folgt:

$$\sqrt{\varkappa_2} = \frac{1-\sqrt{\varkappa'}}{1+\sqrt{\varkappa'}},$$

$$(20)\qquad 4K_2 = (1+\sqrt{\varkappa'})^2 K, \quad K_2' = (1+\sqrt{\varkappa'})^2 K',$$

$$q = \sqrt{\frac{\varkappa_2}{4\varkappa_2'}}\, e^{-\frac{1}{4}\frac{G(\varkappa_2^2)}{F(\varkappa_2^2)}},$$

worin nun der Konvergenzbereich die Ebene der $\varkappa^2$ zweimal (mit einer Verzweigung im Punkte $\varkappa^2 = 1$) bedeckt.

Diese Operation kann man fortsetzen, indem man nach der Formel (17) aus $\varkappa_2$ durch Verdoppelung von ω eine neue Größe $\varkappa_3$, daraus ebenso $\varkappa_4$ usf. herleitet. Man bekommt dann eine Reihe von Ausdrücken für q, deren Konvergenz eine immer bessere wird. Für ein beliebiges ν ist:

$$(21)\qquad q = \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4\varkappa_\nu'}}\, e^{-\frac{G(\varkappa_\nu^2)}{2^\nu F(\varkappa_\nu^2)}}.$$

Die erste Gleichung (18)

$$\varkappa_1 = \frac{\varkappa^2}{(1+\varkappa')^2}$$

zeigt, daß, so lange der absolute Wert von $\varkappa^2$ kleiner als 1 ist, und folglich der absolute Wert von $1+\varkappa'$ größer als 1, der absolute Wert von $\varkappa_1$ kleiner ist als der von $\varkappa^2$, und folglich

nähert sich $\varkappa_\nu$ mit unendlich wachsendem ν der Grenze Null. Daraus erhält man für q die Darstellung:

$$(22) \qquad q = \lim_{\nu=\infty} \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4\varkappa'_\nu}} = \lim \sqrt[2^{\nu-1}]{\frac{\varkappa_\nu}{4}},$$

die bei reellen Werten von $\varkappa$ zur Berechnung geeignet ist.

Aus jeder der Formeln (21) kann man eine Reihenentwickelung von q nach den steigenden Potenzen von $\varkappa_\nu$ herleiten, deren Konvergenz mit wachsendem ν zunimmt. Wendet man insbesondere die Formel (20) an, so erhält man eine Entwickelung, die von Weierstrass in den Monatsberichten der Berliner Akademie vom Jahre 1883 mitgeteilt ist, deren Konvergenzbereich die Ebene $\varkappa^2$ zweimal ausfüllt.

Die Koeffizienten dieser Entwickelung berechnet man am einfachsten aus:

$$(23) \qquad \sqrt{\varkappa_2} = \frac{\vartheta_{10}(0, 4\omega)}{\vartheta_{00}(0, 4\omega)} = \frac{2q + 2q^9 + 2q^{25} + \cdots}{1 + 2q^4 + 2q^{16} + \cdots},$$

und erhält so nach der Methode der unbestimmten Koeffizienten:

$$(24) \qquad q = \frac{\sqrt{\varkappa_2}}{2} + 2\left(\frac{\sqrt{\varkappa_2}}{2}\right)^5 + 15\left(\frac{\sqrt{\varkappa_2}}{2}\right)^9 + 150\left(\frac{\sqrt{\varkappa_2}}{2}\right)^{13} + 1707\left(\frac{\sqrt{\varkappa_2}}{2}\right)^{17} + \cdots$$

Ebenso läßt sich nach (23) auch umgekehrt $\sqrt{\varkappa_2}$ in eine nach Potenzen von q fortschreitende Reihe entwickeln:

$$(25) \qquad \tfrac{1}{2}\sqrt{\varkappa_2} = q - 2q^5 + 5q^9 - 10q^{13} + 18q^{17} \ldots,$$

die man auch durch Umkehrung der Reihe (24) erhält.

Damit ist die am Anfang dieses Paragraphen gestellte Frage vollständig beantwortet.

Bezüglich der Anwendung der hier entwickelten Formeln zu numerischer Berechnung von q sei noch bemerkt, daß, wenn $\varkappa^2$ näher an 1 liegt, man ein besser konvergentes Verfahren erhält, wenn man $\varkappa^2$ mit $\varkappa'^2$ vertauscht. Die Rechnung ergibt dann zunächst nicht q, sondern

$$q' = e^{-\frac{\pi i}{\omega}},$$

woraus man aber q aus der Formel erhält:

$$\log q \log q' = \pi^2.$$

§ 53. Die Lösungen der Gleichung $j(\omega) = j(\omega')$.

Die Resultate von § 51 genügen zunächst, um die Beziehungen der verschiedenen Werte von ω festzustellen, die zu demselben Wert von $\varkappa^2$ führen. Sei also:

$$(1)\qquad \frac{\vartheta_{10}^4(0,\omega')}{\vartheta_{00}^4(0,\omega')} = \frac{\vartheta_{10}^4(0,\omega)}{\vartheta_{00}^4(0,\omega)} = \varkappa^2.$$

Setzen wir

$$(2)\qquad v = \pi\vartheta_{00}^2(0,\omega)u = \pi\vartheta_{00}^2(0,\omega')u',$$

so genügen (nach § 42) sowohl die Funktionen

$$(3)\qquad \frac{\vartheta_{00}(0,\omega)\vartheta_{11}(u,\omega)}{\vartheta_{10}(0,\omega)\vartheta_{01}(u,\omega)},\ \frac{\vartheta_{01}(0,\omega)\vartheta_{10}(u,\omega)}{\vartheta_{10}(0,\omega)\vartheta_{01}(u,\omega)},\ \frac{\vartheta_{01}(0,\omega)\vartheta_{00}(u,\omega)}{\vartheta_{00}(0,\omega)\vartheta_{01}(u,\omega)},$$

als auch

$$(4)\qquad \frac{\vartheta_{00}(0,\omega')\vartheta_{11}(u',\omega')}{\vartheta_{10}(0,\omega')\vartheta_{01}(u',\omega')},\ \frac{\vartheta_{01}(0,\omega')\vartheta_{10}(u',\omega')}{\vartheta_{10}(0,\omega')\vartheta_{01}(u',\omega')},\ \frac{\vartheta_{01}(0,\omega')\vartheta_{00}(u',\omega')}{\vartheta_{00}(0,\omega')\vartheta_{01}(u',\omega')},$$

für x, y, z gesetzt, den Differentialgleichungen (1) des vorigen Paragraphen, und die entsprechenden dieser Funktionen sind also identisch. Wenn nun $u' = \frac{1}{2}$ ist, so verschwindet $\vartheta_{10}(u',\omega')$ und es muß dann auch $\vartheta_{10}(u,\omega)$ verschwinden. Demnach folgt aus (2) mit Rücksicht auf § 21:

$$(5)\qquad \vartheta_{00}^2(0,\omega') = \vartheta_{00}^2(0,\omega)(\alpha + \beta\omega),$$

worin α, β ganze Zahlen sind, die der Bedingung

$$(6)\qquad \alpha \equiv 1,\qquad \beta \equiv 0 \pmod 2$$

genügen. Ist $u' = \omega' : 2$, so verschwinden $\vartheta_{01}(u',\omega')$ und $\vartheta_{01}(u,\omega)$, und daher ist wie oben

$$(7)\qquad \vartheta_{00}^2(0,\omega')\omega' = \vartheta_{00}^2(0,\omega)(\gamma + \delta\omega),$$

worin

$$(8)\qquad \gamma \equiv 0,\qquad \delta \equiv 1 \pmod 2).$$

Daraus folgt:

$$(9)\qquad \omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}.$$

Da aber in gleicher Weise geschlossen werden kann:

$$\vartheta_{00}^2(0,\omega) = \vartheta_{00}^2(0,\omega')(\alpha' + \beta'\omega'),$$
$$\vartheta_{00}^2(0,\omega)\omega = \vartheta_{00}^2(0,\omega')(\gamma' + \delta'\omega'),$$

worin α', β', γ', δ' gleichfalls ganze Zahlen sind, so ergibt die Substitution (5) in diesen Gleichungen:

$$1 = (\alpha + \beta\omega)(\alpha' + \beta'\omega'),$$
$$\omega = (\alpha + \beta\omega)(\gamma' + \delta'\omega').$$

Drückt man in diesen Gleichungen ω' nach (9) durch ω aus, so erhält man

$$1 = \alpha'(\alpha + \beta\omega) + \beta'(\gamma + \delta\omega),$$
$$\omega = \gamma'(\alpha + \beta\omega) + \delta'(\gamma + \delta\omega),$$

und da ω nicht reell ist, so zerfällt jede dieser Gleichungen in zwei andere:

$$\alpha\alpha' + \gamma\beta' = 1, \qquad \beta\alpha' + \delta\beta' = 0,$$
$$\alpha\gamma' + \gamma\delta' = 0, \qquad \beta\gamma' + \delta\delta' = 1.$$

Mithin ist

$$(\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') = 1,$$

und daher, da ω, ω' beide einen positiven imaginären Teil haben müssen, also nach (9) die Determinante $\alpha\delta - \beta\gamma$ positiv sein muß:

$$\alpha\delta - \beta\gamma = 1,$$
$$\alpha = \delta', \qquad \delta = \alpha', \qquad \gamma = -\gamma', \qquad \beta = -\beta'.$$

1. Es hängen also ω, ω' durch eine lineare Transformation, und zwar [nach (6), (8)] durch eine der ersten Klasse (§ 36) miteinander zusammen. Daß auch umgekehrt zwei solche Werte ω, ω' denselben Wert $\varkappa^2$ ergeben, ist bereits oben nachgewiesen.

Ein ähnlicher Satz ergibt sich als unmittelbare Konsequenz hieraus, für die Invariante $j(\omega)$ (§ 46).

2. Die Gleichung:

$$j(\omega') = j(\omega) \tag{10}$$

ist dann und nur dann befriedigt, wenn ω' mit ω durch irgend eine lineare Transformation

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

zusammenhängt, wenn also

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \qquad \alpha\delta - \beta\gamma = 1 \tag{11}$$

ist.

Denn bezeichnen wir die zu ω' gehörigen Werte von $\varkappa^2$, $\varkappa'^2$ mit λ^2, λ'^2, so kann die Gleichung (10) so geschrieben werden:

$$\frac{(1 - \lambda^2\lambda'^2)^3}{\lambda^4\lambda'^4} = \frac{(1 - \varkappa^2\varkappa'^2)^3}{\varkappa^4\varkappa'^4},$$

und ist in bezug auf λ^2 eine Gleichung sechsten Grades, deren Wurzeln

$$\varkappa^2, \quad \varkappa'^2, \quad \frac{1}{\varkappa^2}, \quad \frac{1}{\varkappa'^2}, \quad -\frac{\varkappa'^2}{\varkappa^2}, \quad -\frac{\varkappa^2}{\varkappa'^2}$$

sind. Es findet daher (mit Rücksicht auf § 45) eine der folgenden Beziehungen statt:

$$\lambda^2 = \varkappa^2(\omega), \quad \varkappa^2\left(-\frac{1}{\omega}\right), \quad \varkappa^2(\omega + 1), \quad \varkappa^2\left(\frac{\omega - 1}{\omega}\right),$$
$$\varkappa^2\left(-\frac{1}{\omega + 1}\right), \quad \varkappa^2\left(\frac{\omega}{1 - \omega}\right),$$

wonach aus dem ersten Satze die Richtigkeit des zweiten folgt.

Die Variable ω ist hier immer auf einen positiven imaginären Teil beschränkt, und wenn wir zwei durch eine Gleichung (11) zusammenhängende Zahlen ω, ω' äquivalent nennen, so haben alle mit ω äquivalenten Zahlen einen positiven imaginären Teil. Wir können unseren Satz 2. auch so aussprechen:

3. Die Funktion $j(\omega)$ hat für alle äquivalenten Werte ω und nur für diese einen und denselben Wert[1].

Zu jedem Wert von ω gehört ein bestimmter Wert von $j(\omega)$, und zu jedem Wert von $j(\omega)$ ein Wert von ω und die Gesamtheit der äquivalenten Werte ω'. Wenn also eine einwertige Funktion $\Phi(\omega)$ von ω der Bedingung genügt:

$$\Phi\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = \Phi(\omega),$$

so ist $\Phi(\omega)$ eine einwertige Funktion von $j(\omega)$, und wenn wir also annehmen, daß $\Phi(\omega)$ nur für eine endliche Anzahl von Werten $j(\omega)$ unendlich und nur in endlicher Ordnung unendlich werde, so folgt, daß $\Phi(\omega)$ eine rationale Funktion von $j(\omega)$ ist.

Die Voraussetzung trifft z. B. immer dann zu, wenn $\Phi(\omega)$ mit $j(\omega)$ in einem algebraischen Zusammenhange steht.

§ 54. Die Modulfunktionen.

Es sei $\psi(\omega)$ eine eindeutige Funktion von ω. Wendet man auf ω eine lineare Transformation $S = \begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ an, so geht $\psi(\omega)$ in eine andere Funktion

$$(1) \qquad \psi\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)$$

über, die wir mit $\psi|S$ bezeichnen wollen.

---

[1]) Dieser Satz ist zuerst von Dedekind bewiesen (Crelle, Bd. 83). Dedekind nennt danach die Funktion $\text{val}(\omega) = 3^{-3}2^{-6}j(\omega)$ die Valenz von ω.

Die Funktion $\psi(\omega)$ kann möglicherweise bei gewissen Transformationen S ungeändert bleiben (z. B. immer bei der identischen Transformation). Alle Transformationen, die eine Funktion $\psi(\omega)$ ungeändert lassen, bilden eine Gruppe $\mathfrak{G}$. Denn ist

$$\psi \mid S = \psi, \qquad \psi \mid S_1 = \psi,$$

so ist auch

$$\psi \mid S S_1 = \psi \mid S_1 = \psi.$$

Die Gruppe $\mathfrak{G}$ ist ein Teiler der Gruppe $\mathfrak{L}$ aller linearen Transformationen.

Ist $\mathfrak{G}$ ein Teiler von $\mathfrak{L}$ von endlichem Index $(\mathfrak{L}, \mathfrak{G})$, und $\psi(\omega)$ eine Funktion von ω von der Eigenschaft, daß auch umgekehrt

$$\psi(\omega') = \psi(\omega)$$

einen linearen Zusammenhang

$$\omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

zur Folge hat, in dem $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ eine zu $\mathfrak{G}$ gehörige Transformation ist, so heißt $\psi(\omega)$ eine zur Gruppe $\mathfrak{G}$ gehörige Modulfunktion.

Wir beschränken uns auf die Betrachtung solcher Modulfunktionen, die mit dem Modul $\varkappa^2$, also auch mit $j(\omega)$, in einem algebraischen Zusammenhange stehen.

Unter dieser Voraussetzung läßt sich der folgende allgemeine Satz aussprechen:

Wenn $\psi(\omega)$ zur Gruppe $\mathfrak{G}$ gehört und $\chi(\omega)$ durch die Transformationen von $\mathfrak{G}$ ungeändert bleibt, so ist $\chi(\omega)$ rational durch $\psi(\omega)$ ausdrückbar.

Denn zunächst ist $\chi(\omega)$ eine algebraische Funktion von $\psi(\omega)$, und $\psi(\omega)$ kann als algebraische Funktion von $j(\omega)$ jeden Wert annehmen. Zu jedem Wert von $\psi(\omega)$ gehört aber nach Voraussetzung nur ein Wert von $\chi(\omega)$, und daher ist $\chi(\omega)$ als einwertige algebraische Funktion von $\psi(\omega)$ rational.

Das Studium der in $\mathfrak{L}$ enthaltenen Gruppen und der zu ihnen gehörigen Modulfunktionen bildet den Hauptgegenstand des großen Werkes von Klein und Fricke: „Vorlesungen über die Theorie der elliptischen Modulfunktionen“ (2 Bde., Leipzig, Teubner, 1890, 1892). Wir betrachten hier nur einige ganz spezielle Fälle dieser Gruppen und Funktionen, auf die wir im Verlauf unserer Untersuchungen gestoßen sind.

Eine große Klasse von Teilern der Gruppe $\mathfrak{L}$ mit endlichem Index bilden die sogenannten **Kongruenzgruppen**, die, wenn m irgend eine ganze Zahl ist, durch die vier Kongruenzen

$$\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0 \\ 0, & 1\end{pmatrix} (\mathrm{mod}\, m)$$

charakterisiert sind. Die zu diesen Gruppen gehörigen Modulfunktionen heißen **Kongruenzmoduln** $m$ter Stufe. Für $m = 2$ ist dies die Gruppe $\mathfrak{A}$ (§ 36). Wir werden von den folgenden Sätzen Gebrauch machen:

1. **Der Modul** $\varkappa^2$ ist nach § 52 eine zu dieser Gruppe **gehörige** Modulfunktion; da nach § 36 alle diese Transformationen aus den beiden

$$\begin{pmatrix}1, & 0 \\ 2, & 1\end{pmatrix}, \quad \begin{pmatrix}1, & 2 \\ 0, & 1\end{pmatrix}$$

zusammensetzbar sind, so können wir den Satz aussprechen:

Jede Modulfunktion, die durch die beiden Vertauschungen

$$(\omega, \omega + 2), \quad \left(\omega, \frac{\omega}{1 + 2\omega}\right)$$

ungeändert bleibt, ist eine rationale Funktion von $\varkappa^2$.

2. Die Funktion $\varkappa^2\varkappa'^2$ **gehört** zu der aus der ersten und zweiten Klasse des § 36 gemeinschaftlich gebildeten Gruppe $\mathfrak{A}'$. Diese Gruppe läßt sich durch Wiederholung der beiden Transformationen

$$\begin{pmatrix}1, & 0 \\ 2, & 1\end{pmatrix}, \quad \begin{pmatrix}0, & 1 \\ -1, & 0\end{pmatrix}$$

ableiten, und wir können daher den Satz aussprechen:

Jede Modulfunktion, die durch die beiden Vertauschungen

$$(\omega, \omega + 2), \quad \left(\omega, -\frac{1}{\omega}\right)$$

ungeändert bleibt, ist eine rationale Funktion von $\varkappa^2\varkappa'^2$.

Hieraus folgt noch:

3. **Jede Modulfunktion, die durch** $(\omega, \omega + 2)$ **ungeändert bleibt und durch** $\left(\omega, -\frac{1}{\omega}\right)$ **ihr Zeichen ändert, ist das Produkt von** $(\varkappa'^2 - \varkappa^2)$ **mit einer rationalen Funktion von** $\varkappa^2\varkappa'^2$.

4. Die Invariante $j(\omega)$ gehört zur Gruppe $\mathfrak{L}$ (§ 53) und daher der Satz:

Jede Modulfunktion, die durch die beiden Vertauschungen

$$(\omega, \omega + 1), \qquad \left(\omega, -\frac{1}{\omega}\right)$$

ungeändert bleibt, ist eine rationale Funktion von $j(\omega)$.

Außer diesen führen wir noch zwei andere Modulfunktionen ein.

Aus der Definition der Funktionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ [§ 34, (1), (10)] ergibt sich, wenn man die beiden Gleichungen § 42, (3) miteinander multipliziert:

$$(2) \quad f(\omega) = \frac{\sqrt[6]{2}}{\sqrt[12]{\varkappa\varkappa'}}, \quad f_1(\omega) = \sqrt[6]{2}\sqrt[12]{\frac{\varkappa'^2}{\varkappa}}, \quad f_2(\omega) = \sqrt[6]{2}\sqrt[12]{\frac{\varkappa^2}{\varkappa'}},$$

$$(3) \qquad \frac{f_1(\omega)}{f(\omega)} = \sqrt[4]{\varkappa'}, \qquad \frac{f_2(\omega)}{f(\omega)} = \sqrt[4]{\varkappa}.$$

Auf Grund von § 46, (15), (16) definieren wir zwei Funktionen $\gamma_2(\omega)$, $\gamma_3(\omega)$:

$$(4) \quad \begin{aligned} \gamma_2(\omega) &= \sqrt[3]{j(\omega)} = \sqrt[3]{2}^8\, \frac{1 - \varkappa^2\varkappa'^2}{\sqrt[3]{\varkappa^4\varkappa'^4}}, \\ \gamma_3(\omega) &= \sqrt{j(\omega) - 27.64} = \frac{8(2 + \varkappa^2\varkappa'^2)(\varkappa'^2 - \varkappa^2)}{\varkappa^2\varkappa'^2}, \end{aligned}$$

die nach (2) und (3) als eindeutige Funktionen von ω folgendermaßen darstellbar sind:

$$(5) \quad \begin{aligned} \gamma_2(\omega) &= \frac{f(\omega)^{24} - 16}{f(\omega)^8}, \\ \gamma_3(\omega) &= \frac{[f(\omega)^{24} + 8][f_1(\omega)^8 - f_2(\omega)^8]}{f(\omega)^8}, \end{aligned}$$

wofür man nach den Grundformeln für die f-Funktionen [§ 34, (11), (12)] auch setzen kann:

$$(6) \quad \gamma_2(\omega) = f(\omega)^8 f_1(\omega)^8 + f(\omega)^8 f_2(\omega)^8 - f_1(\omega)^8 f_2(\omega)^8,$$

$$(7) \quad \gamma_3(\omega) = \tfrac{1}{2}[f(\omega)^8 + f_1(\omega)^8][f(\omega)^8 + f_2(\omega)^8][f_1(\omega)^8 - f_2(\omega)^8].$$

Es sind also $x = f^8, -f_1^8, -f_2^8$ die Wurzeln der kubischen Gleichung

$$(8) \qquad x^3 - \gamma_2 x - 16 = 0,$$

und $4\gamma_3^2$ ist die Diskriminante dieser Gleichung.

Bemerkenswert sind auch die Differentialgleichungen:

(9) $$d\varkappa^2 = -d\varkappa'^2 = \pi i \vartheta_{00}^4 \varkappa^2 \varkappa'^2 d\omega \text{ [§ 52, (3)]},$$

(10) $$d\varkappa^2\varkappa'^2 = -\pi i \vartheta_{00}^4 (\varkappa^2 - \varkappa'^2)\varkappa^2\varkappa'^2 d\omega,$$

(11) $$df(\omega)^8 = \frac{\pi i}{3}\vartheta_{00}^4 [f_2(\omega)^8 - f_1(\omega)^8] d\omega,$$

(12) $$d\gamma_2(\omega) = -\frac{2\pi i}{3}\gamma_3(\omega)\eta(\omega)^4 d\omega \text{ [nach (5) und § 34, (10)]},$$

(13) $$dj(\omega) = -2\pi i \gamma_2(\omega)^2 \gamma_3(\omega)\eta(\omega)^4 d\omega.$$

Man erhält sodann für die linearen Fundamentaltransformationen aus § 34, (13), (14), (15):

(14) $$\begin{aligned} \gamma_2(\omega+1) &= e^{-\frac{2\pi i}{3}}\gamma_2(\omega), & \gamma_2\left(-\frac{1}{\omega}\right) &= \gamma_2(\omega), \\ \gamma_3(\omega+1) &= -\gamma_3(\omega), & \gamma_3\left(-\frac{1}{\omega}\right) &= -\gamma_3(\omega), \end{aligned}$$

und aus § 40 findet man allgemein:

(15) $$\begin{aligned} \gamma_2\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) &= \varrho\gamma_2(\omega), \\ \gamma_3\left(\frac{\gamma+\delta\omega}{\alpha+\beta\omega}\right) &= (-1)^{\alpha\gamma+\beta\gamma+\beta\delta}\gamma_3(\omega), \end{aligned}$$

worin ϱ wie in § 40, (3) die Bedeutung hat:

$$\varrho = e^{-\frac{2\pi i}{3}(\alpha\gamma+\beta\delta-\alpha\beta-\alpha^2\beta\delta)}.$$

Es sind dies also Modulfunktionen, und die Gruppen, zu denen sie gehören, sind durch die beiden Kongruenzen charakterisiert:

$$\begin{aligned} -\alpha\beta + \alpha\gamma + \beta\delta - \alpha^2\beta\delta &\equiv 0 \pmod 3, \\ \alpha\gamma + \beta\gamma + \beta\delta &\equiv 0 \pmod 2. \end{aligned}$$

Wir geben hiernach unserem Satz 4. die folgende Ergänzung, die sich aus den Formeln (14) ergibt.

5. Eine Modulfunktion, die durch die beiden Substitutionen

$$(\omega, \omega+1), \qquad \left(\omega, -\frac{1}{\omega}\right)$$

das Zeichen ändert, ist das Produkt von $\gamma_3(\omega)$ mit einer rationalen Funktion von $j(\omega)$.

6. Eine Modulfunktion, die durch die Substitution $\left(\omega, -\frac{1}{\omega}\right)$ ungeändert bleibt und durch $(\omega, \omega+1)$ den Faktor $e^{\mp\frac{2\pi i}{3}}$ annimmt, ist das Produkt von $\gamma_3(\omega)^{\pm 1}$ mit einer rationalen Funktion $j(\omega)$.

7. Eine Modulfunktion, die durch die Substitutionen $\left(\omega, -\frac{1}{\omega}\right)$ das Zeichen ändert und durch $(\omega, \omega+1)$ den Faktor $-e^{\mp\frac{2\pi i}{3}}$ annimmt, ist das Produkt von $\gamma_2(\omega)\gamma_3(\omega)^{\pm 1}$ mit einer rationalen Funktion von $j(\omega)$.

Eingehender werden wir uns mit den Modulfunktionen im zweiten Teil beschäftigen.

§ 55. Darstellung der elliptischen Funktionen durch v und $\varkappa^2$.

Wenn wir das Umkehrproblem der elliptischen Integrale so wie in § 51 als die Aufgabe der Integration der elliptischen Differentialgleichungen fassen, so verlangt es die Darstellung der drei Funktionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ durch die beiden unabhängigen Variablen v, $\varkappa^2$. Diese Aufgabe ist durch § 42 gelöst, aber bezüglich der Variablen $\varkappa^2$ nur implizite. Man kann aber auch Darstellungen finden, in denen $\varkappa^2$ explizite vorkommt, und zwar durch Reihen, die nach Potenzen von v fortschreiten, deren Koeffizienten rationale Funktionen von $\varkappa^2$ sind. Die Koeffizienten dieser Reihen können freilich nicht durch ein allgemeines Gesetz dargestellt, sondern nur sukzessive berechnet werden. Diese Darstellungen verdankt man hauptsächlich Weierstrass[1]).

Die σ-Funktionen können, da sie durchaus endliche und stetige Funktionen von u sind, in unbedingt konvergente Potenzreihen nach u entwickelt werden, und wenn wir daher die in § 45, (2) vorkommenden σ-Funktionen in dieser Weise entwickeln, so bekommen wir eine Lösung unserer Aufgabe. Wir setzen daher

---

[1]) Über die Weierstrasssche Theorie der elliptischen Funktionen vgl. man besonders die von H. A. Schwarz herausgegebenen „Formeln und Lehrsätze zum Gebrauch der elliptischen Funktionen". Über die Reihenentwickelungen vgl. man auch Königsberger, „Vorlesungen über die Theorie der elliptischen Funktionen", 25. Vorlesung.

$$(1)\quad \begin{aligned} \sigma(v, 2K, 2iK') &= \sum_{0,\infty}^{\nu} A_\nu \frac{v^{2\nu+1}}{(2\nu+1)!},\\ \sigma_{00}(v, 2K, 2iK') &= \sum_{0,\infty}^{\nu} B_\nu \frac{v^{2\nu}}{(2\nu)!},\\ \sigma_{01}(v, 2K, 2iK') &= \sum_{0,\infty}^{\nu} C_\nu \frac{v^{2\nu}}{(2\nu)!},\\ \sigma_{10}(v, 2K, 2iK') &= \sum_{0,\infty}^{\nu} D_\nu \frac{v^{2\nu}}{(2\nu)!}, \end{aligned}$$

und die A_ν, B_ν, C_ν, D_ν sind die zu bestimmenden Funktionen von $\varkappa^2$ oder von ω. Fassen wir sie zunächst als Funktionen von ω auf, so ergeben die linearen Transformationen [§ 45, (3)]:

$$(2)\quad \begin{aligned} A_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu A_\nu(\omega),\\ B_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu B_\nu(\omega),\\ C_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu D_\nu(\omega),\\ D_\nu\left(-\frac{1}{\omega}\right) &= (-1)^\nu C_\nu(\omega). \end{aligned}$$

$$(3)\quad \begin{aligned} \varkappa'^{2\nu} A_\nu(\omega+1) &= A_\nu(\omega),\\ \varkappa'^{2\nu} B_\nu(\omega+1) &= C_\nu(\omega),\\ \varkappa'^{2\nu} C_\nu(\omega+1) &= B_\nu(\omega),\\ \varkappa'^{2\nu} D_\nu(\omega+1) &= D_\nu(\omega); \end{aligned}$$

$$(4)\quad \begin{aligned} A_\nu(\omega+2) &= A_\nu(\omega),\\ B_\nu(\omega+2) &= B_\nu(\omega),\\ C_\nu(\omega+2) &= C_\nu(\omega),\\ D_\nu(\omega+2) &= D_\nu(\omega). \end{aligned}$$

Hieraus schließen wir auf die charakteristischen Eigenschaften dieser Koeffizienten als Funktionen von $\varkappa^2$. Zunächst erhellt aus der Bedeutung der Koeffizienten, daß für jeden Wert von $\varkappa^2$ mit etwaiger Ausnahme von $\varkappa^2 = 0, 1, \infty$ die Koeffizienten $A_\nu(\varkappa^2)$, $B_\nu(\varkappa^2)$, $C_\nu(\varkappa^2)$, $D_\nu(\varkappa^2)$ endliche und stetige Funktionen von $\varkappa^2$ sind.

Aber auch für $\varkappa^2 = 0$ bleiben diese Funktionen endlich und man kann ihre Werte leicht finden, wenn man in den Darstellungen des § 37 q und mithin $\varkappa^2$ in Null übergehen läßt.

Man erhält dann aus den Entwickelungen in § 25 mit Rücksicht darauf, daß nach § 34 und § 42 für ein verschwindendes q

$$\eta(\omega) = q^{\frac{1}{12}}, \qquad 2K = \pi$$

wird:

$$(5)\qquad \begin{aligned} e^{\frac{v^2}{6}} \sin v &= \sum_{0,\infty}^{\nu} A_\nu(0) \frac{v^{2\nu+1}}{(2\nu+1)!}, \\ e^{\frac{v^2}{6}} &= \sum_{0,\infty}^{\nu} B_\nu(0) \frac{v^{2\nu}}{(2\nu)!}, \\ e^{\frac{v^2}{6}} &= \sum_{0,\infty}^{\nu} C_\nu(0) \frac{v^{2\nu}}{(2\nu)!}, \\ e^{\frac{v^2}{6}} \cos v &= \sum_{0,\infty}^{\nu} D_\nu(0) \frac{v^{2\nu}}{(2\nu)!}. \end{aligned}$$

Die Formeln (2) ergeben nun:

$$(6)\qquad \begin{aligned} A_\nu(\varkappa'^2) &= (-1)^\nu A_\nu(\varkappa^2), \\ B_\nu(\varkappa'^2) &= (-1)^\nu B_\nu(\varkappa^2), \\ C_\nu(\varkappa'^2) &= (-1)^\nu D_\nu(\varkappa^2), \\ D_\nu(\varkappa'^2) &= (-1)^\nu C_\nu(\varkappa^2), \end{aligned}$$

woraus folgt, daß auch für $\varkappa^2 = 1$ diese Funktionen endlich bleiben, nämlich:

$$(7)\qquad \begin{aligned} A_\nu(1) &= (-1)^\nu A_\nu(0), \\ B_\nu(1) &= (-1)^\nu B_\nu(0), \\ C_\nu(1) &= (-1)^\nu D_\nu(0), \\ D_\nu(1) &= (-1)^\nu C_\nu(0). \end{aligned}$$

Das System (3) läßt sich ferner so schreiben:

$$(8)\qquad \begin{aligned} \varkappa'^{2\nu} A_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= A_\nu(\varkappa^2), \\ \varkappa'^{2\nu} B_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= C_\nu(\varkappa^2), \\ \varkappa'^{2\nu} C_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= B_\nu(\varkappa^2), \\ \varkappa'^{2\nu} D_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) &= D_\nu(\varkappa^2), \end{aligned}$$

woraus für ein unendliches $\varkappa^2$:

$$(9)\qquad \begin{aligned} A_\nu(\varkappa^2) &= \varkappa^{2\nu} A_\nu(0), \\ B_\nu(\varkappa^2) &= \varkappa^{2\nu} D_\nu(0), \\ C_\nu(\varkappa^2) &= \varkappa^{2\nu} B_\nu(0), \\ D_\nu(\varkappa^2) &= \varkappa^{2\nu} C_\nu(0), \end{aligned}$$

und hieraus wird geschlossen, daß die Koeffizienten A_ν, B_ν, C_ν, D_ν ganze rationale Funktionen von $\varkappa^2$ vom Grade ν sind, und aus § 54, 2, 3, folgt überdies noch, daß A_ν, B_ν bei geradem ν rational durch $\varkappa^2\varkappa'^2$ ausgedrückt sind, während sie bei ungeradem ν gleich dem Produkt von $(\varkappa'^2 - \varkappa^2)$ mit einer rationalen Funktion von $\varkappa^2\varkappa'^2$ sind.

Aus B_ν findet man C_ν mittels der Formel:

$$C_\nu(\varkappa^2) = \varkappa'^{2\nu} B_\nu\left(\frac{-\varkappa^2}{\varkappa'^2}\right) \tag{10}$$

und D_ν durch Anwendung von (6) und (8):

$$D_\nu(\varkappa^2) = (-1)^\nu C_\nu(\varkappa'^2) = (-1)^\nu \varkappa^{2\nu} B_\nu\left(\frac{-\varkappa'^2}{\varkappa^2}\right). \tag{11}$$

Da man aus (5) die Koeffizienten $A_\nu(0)$, $B_\nu(0)$, $C_\nu(0)$, $D_\nu(0)$ leicht bestimmen kann, so ergeben sich aus dem hier entwickelten Formelsystem die Koeffizienten A_ν, B_ν, C_ν, D_ν ohne weitere Rechnung bis $\nu = 3$ einschließlich.

Man findet:

$$A_0 = 1, \quad A_1 = 0, \quad A_2 = -\frac{2}{3}(1 - \varkappa^2\varkappa'^2),$$

$$B_0 = 1, \quad B_1 = \frac{1}{3}(\varkappa'^2 - \varkappa^2), \quad B_2 = \frac{1}{3}(1 + 2\varkappa^2\varkappa'^2),$$

$$C_0 = 1, \quad C_1 = \frac{1}{3}(1 + \varkappa^2), \quad C_2 = \frac{1}{3}(\varkappa'^4 - 2\varkappa^2),$$

$$D_0 = 1, \quad D_1 = -\frac{1}{3}(1 + \varkappa'^2), \quad D_2 = \frac{1}{3}(\varkappa^4 - 2\varkappa'^2).$$

$$A_3 = -\frac{8}{9}(\varkappa'^2 - \varkappa^2)(2 + \varkappa^2\varkappa'^2),$$

$$B_3 = \frac{1}{9}(\varkappa'^2 - \varkappa^2)(5 - 2\varkappa^2\varkappa'^2),$$

$$C_3 = \frac{1}{9}(1 + \varkappa^2)(5\varkappa'^4 + 2\varkappa^2),$$

$$D_3 = -\frac{1}{9}(1 + \varkappa'^2)(5\varkappa^4 + 2\varkappa'^2).$$

Weitere Koeffizienten lassen sich auf demselben Wege, wenn auch weitläufiger berechnen, indem man die Ausdrücke für die σ-Funktionen in § 32 nach Potenzen von q entwickelt und, wie hier die niedrigste Potenz von q, so die höheren benutzt. Weierstrass bedient sich zur rekurrenten Berechnung der Koeffizienten gewisser partieller Differentialgleichungen, ähnlich der, die wir im nächsten Paragraphen für die Funktion σ ableiten werden.

§ 56. Potenzreihen für die Weierstrassschen Funktionen $\wp(u)$, $\sigma(u)$.

Die Funktion $\sigma(u)$, als Funktion von u betrachtet, läßt sich, wie schon bemerkt, in eine in der ganzen u-Ebene konvergierende Reihe nach Potenzen von u entwickeln, und nach § 35, (8), (12) hat diese Entwickelung die folgende Form:

(1) $$\sigma(u) = u + \alpha u^3 + \alpha_1 u^5 + \alpha_2 u^7 + \alpha_3 u^9 + \cdots$$

Die Funktion

(2) $$\wp(u) = -\frac{d^2 \log \sigma(u)}{du^2} = \frac{\sigma'(u)^2 - \sigma\sigma''(u)}{\sigma(u)^2}$$

läßt sich ebenfalls nach steigenden Potenzen von u entwickeln, aber nicht mehr in eine immer konvergente Reihe, sondern diese Reihe hat einen Konvergenzkreis. Sie hat die Form:

(3) $$\wp(u) = \frac{1}{u^2} + a + a_1 u^2 + a_2 u^4 + a_3 u^6 + \cdots$$

und man kann die Koeffizienten a, a_1, a_2, a_3, ... der Reihe nach aus der Differentialgleichung [§ 46, (18)]

(4) $$\wp'(u)^2 = 4\wp(u)^3 - g_2 \wp(u) - g_3$$

als Funktionen von g_2, g_3 bestimmen.

Es ist zunächst

$$\wp'(u) = -\frac{2}{u^3} + 2a_1 u + 4a_2 u^3 + 6a_3 u^5 + \cdots,$$

$$\wp'(u)^2 = \frac{4}{u^6} - \frac{8a_1}{u^2} - 16a_2 + (4a_1^2 - 24a_3)u^2 + \cdots,$$

und da $\wp'(u)^2$ kein Glied mit u^{-4} enthält, während in $\wp(u)^3$ das Glied $3au^{-4}$ vorkommt, so muß $a = 0$ sein. Danach ergibt sich:

$$\wp(u)^3 = \frac{1}{u^6} + \frac{3a_1}{u^2} + 3a_2 + 3(a_3 + a_1^2)u^2 + \cdots$$

$$\wp(u) = \frac{1}{u^2} + a_1 u^2 + \cdots$$

Und wenn man dies in die Gleichung (4) einsetzt, so folgt

(5) $$a_1 = \frac{g_2}{20}, \quad a_2 = \frac{g_3}{28}, \quad a_3 = \frac{g_2^2}{1200}.$$

Durch Integration von (2) findet man:

$$\sigma'(u) = \left(\frac{1}{u} - \frac{\alpha_1 u^3}{3} - \frac{\alpha_2 u^5}{5} - \frac{\alpha_3 u^7}{7} \cdots\right) \sigma(u),$$

und aus dieser Gleichung folgt:

$$(6) \qquad \alpha = 0, \quad \alpha_1 = \frac{-g_2}{240}, \quad \alpha_2 = \frac{-g_3}{840}, \quad \alpha_3 = \frac{-g_2^2}{161\,280}.$$

Daß $\alpha = 0$ ist, folgt auch aus dem in § 35 bewiesenen $\sigma'''(u) = 0$; indessen war dies dort auf ziemlich umständlichem Wege bewiesen. Wir haben sonach folgenden Anfang der Entwickelung von $\sigma(u)$, wobei der Übersicht halber die numerischen Nenner in ihre Primfaktoren zerlegt sind:

$$(7) \quad \sigma(u) = u - \frac{g_2}{2^4 . 3 . 5} u^5 - \frac{g_3}{2^3 . 3 . 5 . 7} u^7 - \frac{g_2^2}{2^9 . 3^2 . 5 . 7} u^9 - \cdots$$

Zur rekurrenten Berechnung der Koeffizienten in der Potenzreihe für $\sigma(u)$ dient eine partielle Differentialgleichung, die als eine Umformung der partiellen Differentialgleichung für die ϑ-Funktionen betrachtet werden kann. Wir leiten sie auf folgendem Wege her.

Die Funktion $\sigma(u)$ war durch die beiden Periodengleichungen § 35, (9)

$$(8) \qquad \begin{aligned} \sigma(u + \omega_1) &= -e^{\eta_1(2u+\omega_1)} \sigma(u), \\ \sigma(u + \omega_2) &= -e^{\eta_2(2u+\omega_2)} \sigma(u), \\ \eta_1 \omega_2 - \eta_2 \omega_1 &= \pi i \end{aligned}$$

bis auf einen von u unabhängigen Faktor bestimmt. Es ergibt sich aber durch Differentiation der letzten Gleichung (8):

$$\frac{\partial \eta_1}{\partial \omega_1} \omega_2 - \frac{\partial \eta_2}{\partial \omega_1} \omega_1 - \eta_2 = 0,$$

$$\frac{\partial \eta_1}{\partial \omega_2} \omega_2 - \frac{\partial \eta_2}{\partial \omega_2} \omega_1 + \eta_1 = 0,$$

also:

$$\omega_2 \left(\eta_1 \frac{\partial \eta_1}{\partial \omega_1} + \eta_2 \frac{\partial \eta_1}{\partial \omega_2}\right) = \omega_1 \left(\eta_1 \frac{\partial \eta_2}{\partial \omega_1} + \eta_2 \frac{\partial \eta_2}{\partial \omega_2}\right),$$

und wir führen also eine Größe r ein, die wir so definieren:

$$(9) \qquad \begin{aligned} \eta_1 \frac{\partial \eta_1}{\partial \omega_1} + \eta_2 \frac{\partial \eta_1}{\partial \omega_1} &= -r \omega_1, \\ \eta_1 \frac{\partial \eta_1}{\partial \omega_2} + \eta_2 \frac{\partial \eta_2}{\partial \omega_2} &= -r \omega_2. \end{aligned}$$

Nun weist man durch Differentiation der Periodengleichungen (8) nach, daß die Funktion

$$S(u) = \frac{\partial^2 \sigma}{\partial u^2} + 4\eta_1 \frac{\partial \sigma}{\partial \omega_1} + 4\eta_2 \frac{\partial \sigma}{\partial \omega_2} + 4 r u^2 \sigma$$

den Periodengleichungen (8) genügt, und also gleich $C\sigma(u)$ ist, worin C von u unabhängig ist. Die Entwickelung von $\sigma(u)$ nach Potenzen von u fängt aber mit u^3 an, während $\sigma(u)$ mit u anfängt, und folglich muß $C = 0$ sein.

Nach (7) beginnt die Entwickelung von $\partial\sigma/\partial\omega_1$ und $\partial\sigma/\partial\omega_2$ erst mit u^5, und die ersten Glieder von $\partial^2\sigma/\partial u^2$ und $4ru^2\sigma$ sind $-g_2u^3/12$, $4ru^3$, woraus $4r = g_2/12$ folgt, und demnach erhält die Differentialgleichung für σ die Form:

$$(10) \qquad \frac{\partial^2 \sigma}{\partial u^2} + 4\eta_1 \frac{\partial \sigma}{\partial \omega_1} + 4\eta_2 \frac{\partial \sigma}{\partial \omega_2} + \frac{g_2}{12} u^2 \sigma = 0,$$

und nebenbei ergeben sich aus (9) die Relationen:

$$(11) \qquad \begin{aligned} \eta_1 \frac{\partial \eta_1}{\partial \omega_1} + \eta_2 \frac{\partial \eta_1}{\partial \omega_1} &= -\frac{g_2}{48}\omega_1, \\ \eta_1 \frac{\partial \eta_1}{\partial \omega_2} + \eta_2 \frac{\partial \eta_2}{\partial \omega_2} &= -\frac{g_2}{48}\omega_2. \end{aligned}$$

Nun sollen in der Differentialgleichung (10) statt der Variablen ω_1, ω_2 die Variablen g_2, g_3 eingeführt werden, und wenn wir also

$$\begin{aligned} \frac{\partial \sigma}{\partial \omega_1} &= \frac{\partial \sigma}{\partial g_2}\frac{\partial g_2}{\partial \omega_1} + \frac{\partial \sigma}{\partial g_3}\frac{\partial g_3}{\partial \omega_1}, \\ \frac{\partial \sigma}{\partial \omega_2} &= \frac{\partial \sigma}{\partial g_2}\frac{\partial g_2}{\partial \omega_2} + \frac{\partial \sigma}{\partial g_3}\frac{\partial g_3}{\partial \omega_2} \end{aligned}$$

setzen, so erhält (10) die Form:

$$(12) \qquad \frac{\partial^2 \sigma}{\partial u^2} + h_2 \frac{\partial \sigma}{\partial g_2} + h_3 \frac{\partial \sigma}{\partial g_3} + \frac{g_2}{12} u^2 \sigma = 0,$$

worin

$$\begin{aligned} h_2 &= 4\left(\eta_1 \frac{\partial g_2}{\partial \omega_1} + \eta_2 \frac{\partial g_2}{\partial \omega_2}\right), \\ h_3 &= 4\left(\eta_1 \frac{\partial g_3}{\partial \omega_1} + \eta_2 \frac{\partial g_3}{\partial \omega_2}\right). \end{aligned}$$

Die Größen h_2, h_3, durch g_2, g_3 ausgedrückt, ergeben sich nun aus der Differentialgleichung selbst, wenn man für σ die Entwickelung (7) einsetzt. Danach ist bis zur 7ten Potenz von u:

$$\begin{aligned}
\frac{\partial^2\sigma}{\partial u^2} &= -\frac{g_2}{12}u^3 - 12g_3\frac{u^5}{2^4.3.5} - \frac{3}{8}g_2^2\frac{u^7}{2^3.3.5.7},\\
\frac{\partial\sigma}{\partial g_2} &= \qquad\quad - \frac{u^5}{2^4.3.5}\\
\frac{\partial\sigma}{\partial g_3} &= \qquad\qquad\qquad - \frac{u^7}{2^3.3.5.7},\\
\frac{g_2}{12}u^2\sigma &= \frac{g_2}{12}u^3 \qquad\quad -\frac{7}{24}g_2^2\frac{u^7}{2^3.3.5.7},
\end{aligned}$$

und wenn man dies in (12) einsetzt und die Koeffizienten von u^5 und u^7 gleich Null setzt, so ergibt sich:

$$h_2 = -12g_3, \quad h_3 = -\tfrac{2}{3}g_2^2,$$

und wir erhalten die Differentialgleichung:

$$\frac{\partial^2\sigma}{\partial u^2} - 12g_3\frac{\partial\sigma}{\partial g_2} - \frac{2}{3}g_2^2\frac{\partial\sigma}{\partial g_3} + \frac{g_2}{12}u^2\sigma = 0. \tag{13}$$

Setzt man die Reihenentwickelung für σ mit unbestimmten Koeffizienten an:

$$\sigma = \Sigma A_\nu \frac{u^{2\nu+1}}{(2\nu+1)!}, \tag{14}$$

so erhält man aus (13) die Rekursionsformel:

$$A_\nu = 12g_3\frac{\partial A_{\nu-1}}{\partial g_2} + \frac{2}{3}g_2^2\frac{\partial A_{\nu-1}}{\partial g_3} - \frac{(2\nu-1)(2\nu-2)}{12}g_2^2 A_{\nu-2}, \tag{15}$$

woraus zu schließen ist, daß die A_ν ganze rationale Funktionen von g_2 und g_3 sind, deren Koeffizienten rationale Zahlen sind, die nur Potenzen von 2 und von 3 im Nenner haben können. Die Reihe (14) besteht daher aus Gliedern von der Form

$$a_{m,n}(\tfrac{1}{2}g_2)^m(2g_3)^n\frac{u^{2\nu+1}}{(2\nu+1)!},$$

und aus der Homogenität der Funktion σ [§ 37, (8), § 46, (13)] folgt:

$$2m + 3n = \nu, \tag{16}$$

für die Koeffizienten $a_{m,n}$ ergibt sich dann aus (15):

$$\begin{aligned}
a_{m,n} &= 3(m+1)a_{m+1,\,n-1} + \frac{16}{3}(n+1)a_{m-2,\,n+1}\\
&\quad - \frac{1}{3}(2m+3n-1)(4m+6n-1)a_{m-1,\,n},
\end{aligned} \tag{17}$$

worin $a_{00} = 1$ und die a, bei denen einer der beiden Indizes negativ ist, gleich Null zu setzen sind.

Daraus läßt sich $a_{m,n}$ finden, wenn die früheren $a_{m,n}$, d. h. die in dem $2m + 3n$ kleiner als ν ist, schon berechnet sind.

Man sieht daraus, daß die $a_{m,n}$ nur Potenzen von 3 im Nenner enthalten. In den von H. A. Schwarz herausgegebenen „Formeln und Lehrsätzen zum Gebrauch der elliptischen Funktionen“, nach Vorlesungen von Weierstrass (2. Ausgabe 1893), sind die $a_{m,n}$ bis zu $\nu = 17$ berechnet. Es zeigt sich dabei, daß diese Koeffizienten nicht nur ganze Zahlen sind, sondern daß sie auch mit ν wachsende Potenzen von 3 als Faktoren enthalten. Einen Beweis hierfür vermag ich nicht zu geben.

Sechster Abschnitt.

Multiplikation und Teilung der elliptischen Funktionen.

§ 57. Multiplikation der elliptischen Funktionen.

Unter der Multiplikation der elliptischen Funktionen versteht man die Darstellung der Funktionen $\operatorname{sn} nv$, $\operatorname{cn} nv$, $\operatorname{dn} nv$ für ein ganzzahliges n als rationale Funktionen von $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$, eine Aufgabe, die, wie aus dem Additionstheorem ersichtlich ist, immer gelöst werden kann.

Die Form der Lösung ergibt sich leicht aus der Betrachtung der ϑ-Funktionen.

Es sind, wie aus § 21 unmittelbar zu ersehen, die Funktionen $\vartheta_{g_1, g_2}(nu)$ Θ-Funktionen der Ordnung n^2, deren Charakteristik bei geradem n gleich $(0, 0)$, bei ungeradem n gleich (g_1, g_2) ist. Überdies ist $\vartheta_{11}(nu)$ eine ungerade, $\vartheta_{00}(nu)$, $\vartheta_{10}(nu)$, $\vartheta_{01}(nu)$ sind gerade Funktionen von u. Es lassen sich also diese Funktionen rational durch die ϑ-Funktionen darstellen und die Sätze des § 21 ergeben die Form dieser Ausdrücke. Es wird, wenn wir wieder mit $F^{(\nu)}(x, y)$ eine ganze, rationale, homogene Funktion νter Ordnung bezeichnen:

bei geradem n:

$$(1)\quad \begin{aligned} \vartheta_{11}(nu) &= \vartheta_{00}(u)\,\vartheta_{01}(u)\,\vartheta_{10}(u)\,\vartheta_{11}(u)\,F^{\left(\frac{n^2-4}{2}\right)}[\vartheta_{11}^2(u), \vartheta_{01}^2(u)], \\ \vartheta_{g_1, g_2}(nu) &= F^{\left(\frac{n^2}{2}\right)}[\vartheta_{11}^2(u), \vartheta_{01}^2(u)], \quad (g_1, g_2) = (10), (01), (00); \end{aligned}$$

bei ungeradem n:

$$(2)\qquad \vartheta_{g_1, g_2}(nu) = \vartheta_{g_1, g_2}(u)\,F^{\left(\frac{n^2-1}{2}\right)}[\vartheta_{11}^2(u), \vartheta_{01}^2(u)].$$

Wenn wir diese Formeln durch $\vartheta_{01}(u)^{n^2}$ dividieren, so lassen sich die rechten Seiten als ganze rationale Funktionen von den elliptischen Funktionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ darstellen (§ 42). Wenn wir also

(3) $$v = \pi \vartheta_{00}^2 u, \quad \operatorname{sn} v = x, \quad \operatorname{cn} v = y, \quad \operatorname{dn} v = z$$

setzen, so können wir die Formeln (1), (2), indem wir einen konstanten Faktor passend bestimmen, so schreiben:

I. bei geradem n:

$$\frac{\vartheta_{01}^{n^2}\vartheta_{00}}{\vartheta_{10}}\frac{\vartheta_{11}(nu)}{\vartheta_{01}(u)^{n^2}} = xyz\,A(x^2), \qquad A(0) = n,$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{10}}\frac{\vartheta_{10}(nu)}{\vartheta_{01}(u)^{n^2}} = B(x^2), \qquad B(0) = 1,$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{00}}\frac{\vartheta_{00}(nu)}{\vartheta_{01}(u)^{n^2}} = C(x^2), \qquad C(0) = 1,$$

$$\vartheta_{01}^{n^2-1}\frac{\vartheta_{01}(nu)}{\vartheta_{01}(u)^{n^2}} = D(x^2), \qquad D(0) = 1.$$

II. bei ungeradem n:

$$\frac{\vartheta_{00}\vartheta_{01}^{n^2-1}}{\vartheta_{10}}\frac{\vartheta_{11}(nu)}{\vartheta_{01}(u)^{n^2}} = x\,A(x^2), \qquad A(0) = n,$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{10}}\frac{\vartheta_{10}(nu)}{\vartheta_{01}(u)^{n^2}} = y\,B(x^2), \qquad B(0) = 1,$$

$$\frac{\vartheta_{01}^{n^2}}{\vartheta_{00}}\frac{\vartheta_{00}(nu)}{\vartheta_{01}(u)^{n^2}} = z\,C(x^2), \qquad C(0) = 1,$$

$$\vartheta_{01}^{n^2-1}\frac{\vartheta_{01}(nu)}{\vartheta_{01}(u)^{n^2}} = D(x^2), \qquad D(0) = 1,$$

worin A, B, C, D ganze rationale Funktionen von x^2 sind, deren Grade sich aus den Formeln (1), (2) folgendermaßen ergeben:

$$\begin{array}{llllll} & A(x^2), & B(x^2), & C(x^2), & D(x^2), & \\ \text{Grad:} & \frac{n^2}{2} - 2, & \frac{n^2}{2}, & \frac{n^2}{2}, & \frac{n^2}{2} & n \text{ gerade}, \\ & \frac{n^2-1}{2}, & \frac{n^2-1}{2}, & \frac{n^2-1}{2}, & \frac{n^2-2}{2} & n \text{ ungerade}. \end{array}$$

Aus den Definitionen I., II. erhält man unmittelbar die Werte von $A(0)$, $B(0)$, $C(0)$, $D(0)$, d. h. die von n unabhängigen Glieder, wie sie beigefügt sind.

Mannigfache Beziehungen zwischen diesen Funktionen ergeben sich noch auf folgendem Wege:

Ersetzt man, um ein Beispiel hier ausführlicher durchzuführen, v durch $v + K$, also u durch $u + \frac{1}{2}$, so gehen x, y, z nach § 44, (18) in y/z, $-\varkappa' x/z$, $\varkappa'/z$ über, und man erhält nach § 21, (8) aus der ersten Formel II für ein ungerades n:

$$\frac{\vartheta_{00}\,\vartheta_{01}{}^{n^2-1}}{\vartheta_{10}}\,\frac{\vartheta_{10}(nu)}{\vartheta_{01}(u)^{n^2}}\left(\frac{\vartheta_{01}(u)}{\vartheta_{00}(u)}\right)^{n^2} = (-1)^{\frac{n-1}{2}}\,\frac{y}{z}\,A\left(\frac{y^2}{z^2}\right).$$

Andererseits ist die linke Seite nach der zweiten Gleichung II und nach § 42 gleich

$$\frac{y}{z}\left(\frac{\sqrt{\varkappa'}}{z}\right)^{n^2-1} B(x^2),$$

und folglich:

$$B(x^2) = (-1)^{\frac{n-1}{2}}\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} A\left(\frac{y^2}{z^2}\right).$$

Setzt man darin $x = 1$, $y = 0$, $z = \varkappa'$ oder $x = 0$, $y = 1$, $z = 1$, so folgt:

$$B(1) = (-1)^{\frac{n-1}{2}}\, n\,\sqrt{\varkappa'}^{\,n^2-1}, \qquad A(1) = (-1)^{\frac{n-1}{2}}\sqrt{\varkappa'}^{\,n^2-1}.$$

Man kann ein ganzes System solcher Formeln ableiten, indem man in I und II folgende Substitutionen macht:

$u,$	$x,$	$y,$	$z,$
$u + \frac{1}{2},$	$\frac{y}{z},$	$\frac{-\varkappa' x}{z},$	$\frac{\varkappa'}{z},$
$u + \frac{\omega}{2},$	$\frac{1}{\varkappa x},$	$\frac{-i z}{\varkappa x},$	$\frac{-i y}{x},$
$u + \frac{1+\omega}{2},$	$\frac{z}{\varkappa y},$	$\frac{i \varkappa'}{\varkappa}\,\frac{1}{y},$	$\frac{i \varkappa' x}{y}.$

So erhält man:

$$(4)\quad \begin{aligned}
&\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-4} A\left(\frac{y^2}{z^2}\right) = (-1)^{\frac{n}{2}-1} A(x^2), && A(1) = (-1)^{\frac{n}{2}-1}\, n\sqrt{\varkappa'}^{\,n^2-4},\\
&\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2} B\left(\frac{y^2}{z^2}\right) = (-1)^{\frac{n}{2}} B(x^2), && B(1) = (-1)^{\frac{n}{2}} \sqrt{\varkappa'}^{\,n^2},\\
&\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2} C\left(\frac{y^2}{z^2}\right) = C(x^2), && C(1) = \sqrt{\varkappa'}^{\,n^2},\\
&\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2} D\left(\frac{y^2}{z^2}\right) = D(x^2), && D(1) = \sqrt{\varkappa'}^{\,n^2},
\end{aligned}$$

n gerade.

$$\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} A\left(\frac{y^2}{z^2}\right) = (-1)^{\frac{n-1}{2}} B(x^2), \quad A(1) = (-1)^{\frac{n-1}{2}} \sqrt{\varkappa'}^{\,n^2-1},$$

$$\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} B\left(\frac{y^2}{z^2}\right) = (-1)^{\frac{n-1}{2}} A(x^2), \quad B(1) = (-1)^{\frac{n-1}{2}} n \sqrt{\varkappa'}^{\,n^2-1},$$

$$\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} C\left(\frac{y^2}{z^2}\right) = D(x^2), \quad C(1) = \sqrt{\varkappa'}^{\,n^2-1},$$

$$\left(\frac{z}{\sqrt{\varkappa'}}\right)^{n^2-1} D\left(\frac{y^2}{z^2}\right) = C(x^2), \quad D(1) = \sqrt{\varkappa'}^{\,n^2-1},$$

n ungerade.

$$(\sqrt{\varkappa}\,x)^{n^2-4} A\left(\frac{1}{\varkappa^2 x^2}\right) = (-1)^{\frac{n}{2}-1} A(x^2), \quad A(\infty) = (-1)^{\frac{n}{2}-1} n\,(\sqrt{\varkappa})^{n^2-4},$$

$$(\sqrt{\varkappa}\,x)^{n^2} B\left(\frac{1}{\varkappa^2 x^2}\right) = B(x^2), \quad B(\infty) = \sqrt{\varkappa}^{\,n^2},$$

$$(\sqrt{\varkappa}\,x)^{n^2} C\left(\frac{1}{\varkappa^2 x^2}\right) = C(x^2), \quad C(\infty) = \sqrt{\varkappa}^{\,n^2},$$

$$(\sqrt{\varkappa}\,x)^{n^2} D\left(\frac{1}{\varkappa^2 x^2}\right) = (-1)^{\frac{n}{2}} D(x^2), \quad D(\infty) = (-1)^{\frac{n}{2}} \sqrt{\varkappa}^{\,n^2},$$

n gerade.

$$(\sqrt{\varkappa}\,x)^{n^2-1} A\left(\frac{1}{\varkappa^2 x^2}\right) = (-1)^{\frac{n-1}{2}} D(x^2), \quad A(\infty) = (-1)^{\frac{n-1}{2}} \sqrt{\varkappa}^{\,n^2-1},$$

$$(\sqrt{\varkappa}\,x)^{n^2-1} B\left(\frac{1}{\varkappa^2 x^2}\right) = C(x^2), \quad B(\infty) = \sqrt{\varkappa}^{\,n^2-1},$$

$$(\sqrt{\varkappa}\,x)^{n^2-1} C\left(\frac{1}{\varkappa^2 x^2}\right) = B(x^2), \quad C(\infty) = \sqrt{\varkappa}^{\,n^2-1},$$

$$(\sqrt{\varkappa}\,x)^{n^2-1} D\left(\frac{1}{\varkappa^2 x^2}\right) = (-1)^{\frac{n-1}{2}} A(x^2), \quad D(\infty) = (-1)^{\frac{n-1}{2}} n \sqrt{\varkappa}^{\,n^2-1},$$

n ungerade.

Hier sind unter $A(\infty)$, $B(\infty)$, $C(\infty)$, $D(\infty)$ jedesmal die Koeffizienten der höchsten Potenz von x in diesen Funktionen zu verstehen. In (7) können die beiden letzten Formeln aus der ersten durch Vertauschung von x mit $1/\varkappa x$ hergeleitet werden.

Das dritte System von Formeln kann man entweder auf demselben Wege oder auch dadurch erhalten, daß man in den Formeln (4), (5) x durch $1/\varkappa x$ ersetzt und (6), (7) anwendet.

$$
(8)\qquad
\begin{aligned}
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2-4} A\left(\frac{z^2}{\varkappa^2 y^2}\right) &= A(x^2), & A\left(\frac{1}{\varkappa^2}\right) &= n\sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-4},\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2} B\left(\frac{z^2}{\varkappa^2 y^2}\right) &= (-1)^{\frac{n}{2}} B(x^2), & B\left(\frac{1}{\varkappa^2}\right) &= (-1)^{\frac{n}{2}}\sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-4},\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2} C\left(\frac{z^2}{\varkappa^2 y^2}\right) &= C(x^2), & C\left(\frac{1}{\varkappa^2}\right) &= \sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-4},\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{2} D\left(\frac{z^2}{\varkappa^2 y^2}\right) &= (-1)^{\frac{n}{2}} D(x^2), & D\left(\frac{1}{\varkappa^2}\right) &= (-1)^{\frac{n}{2}}\sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-4},
\end{aligned}
$$

n gerade.

$$
(9)\qquad
\begin{aligned}
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2-1} A\left(\frac{z^2}{\varkappa^2 y^2}\right) &= (-1)^{\frac{n-1}{2}} C(x^2), & A\left(\frac{1}{\varkappa^2}\right) &= (-1)^{\frac{n-1}{2}}\sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-}\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2-1} B\left(\frac{z^2}{\varkappa^2 y^2}\right) &= D(x^2), & B\left(\frac{1}{\varkappa^2}\right) &= \sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-}\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2-1} C\left(\frac{z^2}{\varkappa^2 y^2}\right) &= (-1)^{\frac{n-1}{2}} A(x^2), & C\left(\frac{1}{\varkappa^2}\right) &= (-1)^{\frac{n-1}{2}} n\sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-}\\
\left(y\sqrt{\frac{\varkappa}{\varkappa'}}\right)^{n^2-1} D\left(\frac{z^2}{\varkappa^2 y^2}\right) &= B(x^2), & D\left(\frac{1}{\varkappa^2}\right) &= \sqrt{\frac{\varkappa'}{\varkappa}}^{\,n^2-}
\end{aligned}
$$

n ungerade.

Nach diesen Formeln kann man für den Fall eines ungeraden n die vier Polynome $A(x^2)$, $B(x^2)$, $C(x^2)$, $D(x^2)$ auf eines von ihnen, z. B. auf $A(x^2)$, zurückführen.

Wenn man von den Formeln I, II je die drei ersten durch die letzte dividiert, so erhält man die Multiplikationsformeln für die elliptischen Funktionen (§ 42).

III. Bei geradem n:

$$
\operatorname{sn} nv = \frac{xyz\,A(x^2)}{D(x^2)},\qquad
\operatorname{cn} nv = \frac{B(x^2)}{D(x^2)},\qquad
\operatorname{dn} nv = \frac{C(x^2)}{D(x^2)},
$$

IV: Bei ungeradem n:

$$
\operatorname{sn} nv = \frac{x\,A(x^2)}{D(x^2)},\qquad
\operatorname{cn} nv = \frac{y\,B(x^2)}{D(x^2)},\qquad
\operatorname{dn} nv = \frac{z\,C(x^2)}{D(x^2)}.
$$

Die Koeffizienten von A, B, C, D hängen noch von ω oder von $\varkappa^2$ ab. Über die Art dieser Abhängigkeit geben die Rekursionsformeln Aufschluß, die man zur sukzessiven Berechnung von

A, B, C, D aus dem Additionstheorem folgert. Wenn wir den Wert des Multiplikators n, zu dem diese Funktionen gehören, durch einen Index andeuten, so haben wir zunächst

$$A_1 = 1, \quad B_1 = 1, \quad C_1 = 1, \quad D_1 = 1; \tag{10}$$

ferner aus den Additionsformeln [§ 44, (16), für $u = v$]:

$$\begin{aligned} \operatorname{sn} 2v &= \frac{2 \operatorname{sn} v \operatorname{cn} v \operatorname{dn} v}{1 - \varkappa^2 \operatorname{sn}^4 v}, \\ \operatorname{cn} 2v &= \frac{\operatorname{cn}^2 v - \operatorname{sn}^2 v \operatorname{dn}^2 v}{1 - \varkappa^2 \operatorname{sn}^4 v}, \\ \operatorname{dn} 2v &= \frac{\operatorname{dn}^2 v - \varkappa^2 \operatorname{sn}^2 v \operatorname{cn}^2 v}{1 - \varkappa^2 \operatorname{sn}^4 v}. \end{aligned} \tag{11}$$

$$\begin{aligned} A_2 &= 2, \\ B_2 &= 1 - 2x^2 + \varkappa^2 x^4, \\ C_2 &= 1 - 2\varkappa^2 x^2 + \varkappa^2 x^4, \\ D_2 &= 1 - \varkappa^2 x^4. \end{aligned} \tag{12}$$

Wenn wir in (11) v durch nv ersetzen, so folgt:

$$\begin{aligned} A_{2n} &= 2 A_n B_n C_n D_n, \\ B_{2n} &= B_n^2 D_n^2 - x^2 y^2 z^2 A_n^2 C_n^2, && n \text{ gerade}, \\ &= y^2 B_n^2 D_n^2 - x^2 z^2 A_n^2 C_n^2, && n \text{ ungerade}, \\ C_{2n} &= C_n^2 D_n^2 - \varkappa^2 x^2 y^2 z^2 A_n^2 B_n^2, && n \text{ gerade}, \\ &= z^2 C_n^2 D_n^2 - \varkappa^2 x^2 y^2 A_n^2 B_n^2, && n \text{ ungerade}, \\ D_{2n} &= D_n^4 - \varkappa^2 x^4 y^4 z^4 A_n^4, && n \text{ gerade}, \\ &= D_n^4 - \varkappa^2 x^4 A_n^4, && n \text{ ungerade}, \end{aligned} \tag{13}$$

und wenn man in den Additionsformeln des § 44 $u = nv$, $v = (n+1)v$ setzt:

$$\begin{aligned} A_{2n+1} &= y^2 z^2 A_n D_n B_{n+1} C_{n+1} + A_{n+1} D_{n+1} C_n B_n, && n \text{ gerade}, \\ &= A_n D_n B_{n+1} C_{n+1} + y^2 z^2 A_{n+1} D_{n+1} C_n B_n, && n \text{ ungerade}, \\ B_{2n+1} &= B_n B_{n+1} D_n D_{n+1} - x^2 z^2 A_n A_{n+1} C_n C_{n+1}, \\ C_{2n+1} &= C_n C_{n+1} D_n D_{n+1} - \varkappa^2 x^2 y^2 A_n A_{n+1} B_n B_{n+1}, \\ D_{2n+1} &= D_n^2 D_{n+1}^2 - \varkappa^2 x^4 y^2 z^2 A_n^2 A_{n+1}^2. \end{aligned} \tag{14}$$

Aus diesen Formeln schließt man, *daß die A, B, C, D ganze rationale Funktionen von $\varkappa^2$ sind, und daß die Zahlenkoeffizienten ganze rationale Zahlen sind.*

Denn nach (10), (12) hat diese Eigenschaft für $n = 1, 2$ statt und folglich nach (13), (14) allgemein.

Über den Grad in bezug auf $\varkappa^2$ läßt sich noch schließen, daß die Koeffizienten von $x^{2\nu}$ den Grad ν in bezug auf $\varkappa^2$ nicht übersteigen. Denn ist diese Regel richtig für n und $n+1$, so folgt ihre Richtigkeit für $2n$ und $2n+1$, und für $n=1$, $n=2$ trifft sie zu.

Aus den Grundgleichungen zwischen den drei elliptischen Funktionen:

$$1 = \mathrm{cn}^2 v + \mathrm{sn}^2 v = \mathrm{dn}^2 v + \varkappa^2 \mathrm{sn}^2 x$$

ergeben sich noch die Relationen:

$$(15)\quad \begin{aligned} D^2 &= B^2 + x^2y^2z^2A^2 = C^2 + \varkappa^2x^2y^2z^2A^2, \quad n \text{ gerade,}\\ D^2 &= y^2B^2 + x^2A^2 \quad = z^2C^2 + \varkappa^2x^2A^2, \quad n \text{ ungerade,}\end{aligned}$$

mit deren Hilfe man nach (14) B_{2n} und C_{2n} durch A_n und D_n allein so ausdrücken kann:

$$(16)\quad \left.\begin{aligned} B_{2n} &= D_n^4 - 2x^2y^2z^2A_n^2D_n^2 + \varkappa^2x^4y^4z^4A_n^4\\ C_{2n} &= D_n^4 - 2\varkappa^2x^2y^2z^2A_n^2D_n^2 + \varkappa^2x^4y^4z^4A_n^4\end{aligned}\right\} n \text{ gerade,}$$
$$\left.\begin{aligned} B_{2n} &= D_n^4 - 2x^2A_n^2D_n^2 + \varkappa^2x^4A_n^4\\ C_{2n} &= D_n^4 - 2\varkappa^2x^2A_n^2D_n^2 + \varkappa^2x^4A_n^4\end{aligned}\right\} n \text{ ungerade.}$$

§ 58. Multiplikation der Funktion $\wp(u)$.

Eine sehr elegante Form erhält die Multiplikationstheorie für die Weierstrasssche Funktion $\wp(u)$ mit den beiden Perioden ω_1, ω_2.

Betrachten wir die doppelt periodische Funktion

$$(1)\qquad \wp(nu) - \wp(u),$$

worin n eine beliebige positive ganze Zahl sein mag. Diese Funktion wird unendlich für $u=0$, und zwar so, daß

$$(2)\qquad \wp(nu) - \wp(u) + \frac{n^2-1}{n^2}\frac{1}{u^2}$$

für $u=0$ endlich bleibt. Außerdem wird sie aber unendlich für alle Werte u^* von u, die der Bedingung

$$nu^* \equiv 0 \pmod{\omega_1, \omega_2}$$

genügen, also von der Form sind:

$$(3)\qquad u^* = \frac{\nu_1\omega_1 + \nu_2\omega_2}{n},$$

worin ν_1, ν_2 beliebige ganze Zahlen bedeuten. Wir erhalten alle in (3) enthaltenen inkongruenten Werte, wenn wir ν_1 und ν_2 je ein vollständiges Restsystem nach dem Modul n durchlaufen lassen.

Die Funktion (1) verschwindet für alle von Null verschiedenen Werte u^0 von u, die der Bedingung

$$\pm n u^0 \equiv u^0 \pmod{\omega_1, \omega_2}$$

genügen, also für

$$u^0 = \frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n \pm 1}, \tag{4}$$

wenn wieder ν_1, ν_2 beliebige ganze Zahlen sind. Die Nullpunkte sind von der ersten, die Unendlichkeitspunkte von der zweiten Ordnung.

Wir führen daher jetzt eine Funktion $\psi_n(u)$ ein, die wir folgendermaßen erklären:

$$\psi_n(u)^2 = n^2 \prod^{\nu_1, \nu_2} \left[\wp(u) - \wp\left(\frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n}\right)\right], \tag{5}$$

wobei ν_1, ν_2 je ein vollständiges Restsystem nach dem Modul n, mit alleinigem Ausschluß des Wertepaares 0,0 durchlaufen, und fügen noch die Bestimmung hinzu, daß $\psi_1 = 1$ sein soll.

Wenn n ungerade ist, so kommt in dem Produkt (5) jeder Linearfaktor zweimal vor, da die beiden inkongruenten Werte

$$u = \pm \frac{\nu_1 \omega_1 + \nu_2 \omega_2}{n}$$

den gleichen Wert von $\wp(u)$ ergeben. Ist aber n gerade, so kommen wieder in (5) alle Linearfaktoren zweimal vor, mit Ausnahme der drei

$$\wp(u) - \wp\left(\frac{\omega_1}{2}\right), \quad \wp(u) - \wp\left(\frac{\omega_2}{2}\right), \quad \wp(u) - \wp\left(\frac{\omega_1 + \omega_2}{2}\right),$$

die nur einfach vorkommen. Beachtet man nun, daß nach § 41

$$\wp'(u)^2 = 4\left[\wp(u) - \wp\left(\frac{\omega_1}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_2}{2}\right)\right]\left[\wp(u) - \wp\left(\frac{\omega_1 + \omega_2}{2}\right)\right]$$

ist, so ergibt sich das Resultat:

$$\begin{aligned} &n \text{ ungerade:} \quad \psi_n = P_n, \\ &n \text{ gerade:} \quad \psi_n = \wp'(u) P_n, \end{aligned} \tag{6}$$

wenn P_n eine ganze rationale Funktion von $\wp(u)$ bedeutet, die bei ungeradem n vom Grade $\frac{1}{2}(n^2 - 1)$ und bei geradem n vom Grade $\frac{1}{2}(n^2 - 4)$ ist, und in der das Glied höchster Ordnung bzw. gleich

$$n\, \wp(u)^{\frac{n^2-1}{2}}, \qquad -\frac{n}{2}\, \wp(u)^{\frac{n^2-4}{2}}$$

ist, wodurch zugleich das nach (5) noch unbestimmte Vorzeichen bestimmt ist. Bei dieser Bestimmung der Vorzeichen ist das Anfangsglied in der Entwickelung von $\psi_n(u)$ nach steigenden Potenzen von u in beiden Fällen (§ 56):

$$\frac{n}{u^{n^2-1}}. \tag{7}$$

Erwägt man nun, daß die Unendlichkeitspunkte der Funktion (1) mit den Nullpunkten von $\psi_n(u)$ zusammenfallen und die Nullpunkte von (1) mit den Nullpunkten von $\psi_{n\pm 1}(u)$, daß also

$$\frac{\psi_n(u)^2[\wp(nu) - \wp(u)]}{\psi_{n+1}(u)\,\psi_{n-1}(u)} \tag{8}$$

eine überall endliche doppelt periodische Funktion und daher eine Konstante ist, deren Wert sich aus $u = 0$ gleich -1 ergibt, so folgt:

$$\wp(nu) = \wp(u) - \frac{\psi_{n+1}(u)\,\psi_{n-1}(u)}{\psi_n(u)^2}, \tag{9}$$

woraus sich die beiden folgenden Formeln ergeben:

$$\begin{aligned} \wp(nu) &= \wp(u) - \frac{P_{n+1}P_{n-1}}{\wp'(u)^2 P_n^2}, \quad n \text{ gerade,} \\ &= \wp(u) - \frac{\wp'(u)^2 P_{n+1}P_{n-1}}{P_n^2}, \quad n \text{ ungerade.} \end{aligned} \tag{10}$$

Wir bestimmen zunächst die Funktion P_n in den ersten Fällen $n = 1, 2, 3, 4$. Dazu bilden wir nach dem Additionstheorem der $\wp$-Funktion [§ 49, (11)]:

$$4[\wp(u) + \wp(v) + \wp(u+v)] = \left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2,$$

indem wir $u = v$ setzen und den Grenzwert rechts durch Differentiation bestimmen:

$$\wp(2u) + 2\wp(u) = \frac{1}{4}\left(\frac{\wp''(u)}{\wp'(u)}\right)^2 = \frac{\frac{1}{4}\left(6\wp(u)^2 - \frac{1}{2}g_2\right)^2}{4\wp(u)^3 - g_2\wp(u) - g_3},$$

oder

$$\wp(2u) = \wp(u) - \frac{3\wp(u)^4 - \frac{3}{2}g_2\wp(u)^2 - 3g_3\wp(u) - \frac{g_2^2}{16}}{\wp'(u)^2}, \tag{11}$$

so daß

$$\psi_1 = 1, \quad \psi_2 = -\wp'(u), \quad \psi_3 = P_3,$$

$$(12)\quad P_1 = 1,\ P_2 = -1,\ P_3 = 3\wp(u)^4 - \frac{3}{2} g_2 \wp(u)^2 - 3 g_3 \wp(u) - \frac{g_2^2}{16}$$

wird. Wir erhalten ferner aus der Additionsformel (§ 49):

$$\wp(v+u) - \wp(v-u) = -\frac{\wp'(u)\,\wp'(v)}{[\wp(v) - \wp(u)]^2},$$

indem wir $v = 2u$ setzen, nach (9):

$$\wp(3u) - \wp(u) = -\frac{\wp'(u)\,\wp'(2u)}{[\wp(2u) - \wp(u)]^2} = -\frac{\wp'(u)^5\,\wp'(2u)}{\psi_3(u)^2},$$

$$= -\frac{\psi_2(u)\,\psi_4(u)}{\psi_3(u)^2},$$

also:

$$\psi_4(u) = \wp'(u) P_4 = -\wp'(u)^4\,\wp'(2u),$$

und wenn man aus (11) den Wert $\wp'(2u)$ bildet:

$$(13)\qquad P_4 = -2\wp(u)^6 + \frac{5}{2} g_2 \wp(u)^4 + 10 g_3 p(u)^3$$

$$+ \frac{5}{8} g_2^2 \wp(u)^2 + \frac{1}{2} g_2 g_3 \wp(u) + g_3^2 - \frac{g_2^3}{32}.$$

Für größere Werte von n leiten wir Rekursionsformeln ab. Zu diesem Zweck wenden wir die Formel (9) auf zwei verschiedene Zahlen m, n an und erhalten:

$$\wp(u) - \wp(mu) = \frac{\psi_{m+1}(u)\,\psi_{m-1}(u)}{\psi_m(u)^2},$$

$$\wp(u) - \wp(nu) = \frac{\psi_{n+1}(u)\,\psi_{n-1}(u)}{\psi_n(u)^2},$$

woraus zu ersehen ist, daß die rechten Seiten einander gleich werden für solche Werte u^0 von u, die von Null verschieden sind und der Bedingung genügen

$$mu^0 \equiv \pm n u^0 \pmod{\omega_1, \omega_2},$$

oder

$$(m \pm n) u^0 \equiv 0 \pmod{\omega_1, \omega_2};$$

für dieselben Werte u^0 verschwinden aber auch die Funktionen

$$\psi_{m \pm n}(u),$$

so daß die beiden Funktionen:

$$\psi_{m+1}(u)\,\psi_{m-1}(u)\,\psi_n(u)^2 - \psi_{n+1}(u)\,\psi_{n-1}(u)\,\psi_m(u)^2,$$

$$\psi_{m+n}(u)\,\psi_{m-n}(u),$$

die nach (6) ganze rationale Funktionen von $\wp(u)$ sind, für die nämlichen endlichen Werte von $\wp(u)$ verschwinden. Sie unter-

scheiden sich also nur durch einen konstanten Faktor voneinander, der sich aus (7) gleich 1 ergibt. Wir haben daher

$$(14)\quad \begin{aligned} &\psi_{m+n}(u)\,\psi_{m+n}(u) \\ &= \psi_{m+1}(u)\,\psi_{m-1}(u)\,\psi_n(u)^2 - \psi_{n+1}(u)\,\psi_{n-1}(u)\,\psi_m(u)^2. \end{aligned}$$

Diese Formel wenden wir auf zwei spezielle Fälle an, indem wir $n+1$, n oder $n+1$, $n-1$ an Stelle von m, n setzen, und erhalten so:

$$\psi_{2n+1}(u) = \psi_{n+2}(u)\,\psi_n(u)^3 - \psi_{n+1}(u)^3\,\psi_{n-1}(u)$$

$$\wp'(u)\,\psi_{2n}(u) = -\psi_n(u)[\psi_{n+2}(u)\,\psi_{n-1}(u)^2 - \psi_{n+1}(u)^2\,\psi_{n-2}(u)],$$

und daraus erhält man nach (6) die Rekursionsformeln für P_n:

$$(15)\quad \begin{aligned} P_{2n+1} &= \wp'(u)^4 P_{n+2} P_n^3 - P_{n+1}^3 P_{n-1}, \quad n \text{ gerade}, \\ &= P_{n+2} P_n^3 - \wp'(u)^4 P_{n+1}^3 P_{n-1}, \quad n \text{ ungerade}. \end{aligned}$$

$$(16)\quad P_{2n} = -P_n(P_{n+2} P_{n-1}^2 - P_{n+1}^2 P_{n-2}).$$

Da sich die Funktionen P_n alle hiernach aus P_1, P_2, P_3, P_4 berechnen lassen, so folgt, daß die Koeffizienten von P_n rational aus g_2, g_3 und rationalen Zahlen zusammengesetzt sind.

Unsere ferneren Betrachtungen über die Teilung knüpfen wir aber an die Multiplikationsformeln der Funktionen $\operatorname{sn} u$, $\operatorname{cn} u$, $\operatorname{dn} u$, deren Vorzüge erst im vierten Teil vollständig zur Geltung kommen werden.

§ 59. Die Teilung durch 2.

Indem wir uns zunächst zur Betrachtung des einfachsten Falles wenden, setzen wir in den Gleichungen (5) des § 57 v an Stelle von $2v$. Dann ist, wenn wir

$$(1)\quad x = \operatorname{sn}\frac{v}{2}, \qquad y = \operatorname{cn}\frac{v}{2}, \qquad z = \operatorname{dn}\frac{v}{2}$$

setzen:

$$(2)\quad \begin{aligned} \operatorname{sn} v &= \frac{2xyz}{1 - \varkappa^2 x^4}, \\ \operatorname{cn} v &= \frac{y^2 - x^2 z^2}{1 - \varkappa^2 x^4}, \\ \operatorname{dn} v &= \frac{z^2 - \varkappa^2 x^2 y^2}{1 - \varkappa^2 x^4}. \end{aligned}$$

Die beiden letzten dieser Gleichungen sind quadratisch in bezug auf x^2, sie haben aber nur eine gemeinschaftliche Wurzel, denn die Wurzeln der zweiten der Gleichungen (2) sind

$$\mathrm{sn}^2\frac{v}{2},\qquad \mathrm{sn}^2\left(\frac{v}{2}+K+iK'\right),$$

und die der dritten

$$\mathrm{sn}^2\frac{v}{2},\qquad \mathrm{sn}^2\left(\frac{v}{2}+K\right).$$

Man findet nun leicht aus (2):

$$1+\mathrm{cn}\,v=\frac{2y^2}{1-\varkappa^2x^4},\qquad 1+\mathrm{dn}\,v=\frac{2z^2}{1-\varkappa^2x^4},$$

$$1-\mathrm{cn}\,v=\frac{2x^2z^2}{1-\varkappa^2x^4},\qquad 1-\mathrm{dn}\,v=\frac{2\varkappa^2x^2y^2}{1-\varkappa^2x^4},$$

$$\mathrm{dn}\,v+\mathrm{cn}\,v=\frac{2y^2z^2}{1-\varkappa^2x^4},$$

also

$$(3)\qquad \begin{aligned} x&=\sqrt{\frac{1-\mathrm{cn}\,v}{1+\mathrm{dn}\,v}}=\frac{1}{\varkappa}\sqrt{\frac{1-\mathrm{dn}\,v}{1+\mathrm{cn}\,v}},\\ y&=\sqrt{\frac{\mathrm{dn}\,v+\mathrm{cn}\,v}{1+\mathrm{dn}\,v}},\quad z=\sqrt{\frac{\mathrm{dn}\,v+\mathrm{cn}\,v}{1+\mathrm{cn}\,v}};\end{aligned}$$

zwischen den Vorzeichen dieser drei Größen besteht nach der ersten Gleichung (2) noch eine Relation, so daß man nur vier verschiedene Wertsysteme erhält, welche folgende Bedeutung haben:

$$\mathrm{sn}\left(\frac{v}{2}\right),\qquad \mathrm{cn}\left(\frac{v}{2}\right),\qquad \mathrm{dn}\left(\frac{v}{2}\right),$$

$$\mathrm{sn}\left(\frac{v}{2}+2K\right),\qquad \mathrm{cn}\left(\frac{v}{2}+2K\right),\qquad \mathrm{dn}\left(\frac{v}{2}+2K\right),$$

$$\mathrm{sn}\left(\frac{v}{2}+2iK'\right),\qquad \mathrm{cn}\left(\frac{v}{2}+2iK'\right),\qquad \mathrm{dn}\left(\frac{v}{2}+2iK'\right),$$

$$\mathrm{sn}\left(\frac{v}{2}+2K+2iK'\right),\quad \mathrm{cn}\left(\frac{v}{2}+2K+2iK'\right),\quad \mathrm{dn}\left(\frac{v}{2}+2K+2iK'\right).$$

Wir führen noch die aus (3) sich ergebenden speziellen Fälle an:

$$\mathrm{sn}\frac{K}{2}=\frac{1}{\sqrt{1+\varkappa'}},\quad \mathrm{sn}\frac{iK'}{2}=\frac{i}{\sqrt{\varkappa}},\quad \mathrm{sn}\frac{K+iK'}{2}=\sqrt{\frac{\varkappa+i\varkappa'}{\varkappa}},$$

$$\mathrm{cn}\frac{K}{2}=\sqrt{\frac{\varkappa'}{1+\varkappa'}},\quad \mathrm{cn}\frac{iK'}{2}=\sqrt{\frac{1+\varkappa}{\varkappa}},\quad \mathrm{cn}\frac{K+iK'}{2}=\sqrt{\frac{-i\varkappa'}{\varkappa}},$$

$$\mathrm{dn}\frac{K}{2}=\sqrt{\varkappa'},\quad \mathrm{dn}\frac{iK'}{2}=\sqrt{1+\varkappa},\quad \mathrm{dn}\frac{K+iK'}{2}=\sqrt{\frac{\varkappa}{\varkappa+i\varkappa'}}.$$

Hieraus folgt nun, daß man die Teilung durch 2 und mithin auch durch jede Potenz von 2 durch eine Kette von Quadratwurzeln ausführen kann. Setzt man daher die Aufgabe der Teilung durch eine ungerade Zahl als gelöst voraus, so ist die Teilung durch eine gerade Zahl auf Quadratwurzeln zurückgeführt. Im folgenden beschäftigen wir uns ausschließlich mit der Teilung durch ungerade Zahlen.

§ 60. Die Teilung durch eine ungerade Zahl.

Setzt man, wenn n eine ungerade Zahl ist,

$$(1) \qquad x = \operatorname{sn}\frac{v}{n}, \qquad y = \operatorname{cn}\frac{v}{n}, \qquad z = \operatorname{dn}\frac{v}{n},$$

so erhält man aus den Gleichungen IV, § 57:

$$(2) \qquad \begin{aligned} D(x^2)\operatorname{sn} v - xA(x^2) &= 0, \\ D(x^2)\operatorname{cn} v - yB(x^2) &= 0, \\ D(x^2)\operatorname{dn} v - zC(x^2) &= 0. \end{aligned}$$

Die erste dieser Gleichungen ist in bezug auf die Unbekannte x vom Grade n^2; durch die zweite und dritte werden y und z rational durch x (und durch $\operatorname{cn} v$, $\operatorname{dn} v$) ausgedrückt. Es ergeben sich also n^2 Wertsysteme für die drei Unbekannten x, y, z, deren Bedeutung ist:

$$(3) \qquad \begin{aligned} x_{\mu,\mu'} &= \operatorname{sn}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right), \\ y_{\mu,\mu'} &= \operatorname{cn}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right), \\ z_{\mu,\mu'} &= \operatorname{dn}\left(\frac{v}{n} + \frac{4\mu K + 4\mu' iK'}{n}\right), \end{aligned}$$

worin μ, μ' je ein vollständiges Restsystem (mod n) durchlaufen.

Die erste Gleichung (2):

$$(4) \qquad D(x^2)\operatorname{sn} v - xA(x^2) = 0,$$

vom Grade n^2 heißt die allgemeine Teilungsgleichung. Sie ist in dem Sinne irreducibel, daß sie nicht in Faktoren zerlegbar ist, die in bezug auf $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ rational sind und beliebige von v unabhängige Koeffizienten haben.

Denn zunächst sind die n^2 Werte $x_{\mu,\mu'}$ alle voneinander verschieden, und wenn irgend eine rationale Gleichung:

$$F\left(\operatorname{sn}\frac{v}{n}, \operatorname{sn} v, \operatorname{cn} v, \operatorname{dn} v\right) = 0$$

besteht, so kann darin die Variable v durch $v + 4\mu K + 4\mu' i K'$ ersetzt werden. Wegen der Periodizität von $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$ folgt aber daraus, daß die Gleichung

$$F(x, \operatorname{sn} v, \operatorname{cn} v, \operatorname{dn} v) = 0$$

für alle Wurzeln der Gleichung (4) erfüllt ist. Um ihre Galoissche Gruppe zu ermitteln, setzen wir zunächst den Rationalitätsbereich fest. Er soll folgende Größen umfassen:

1. rationale Zahlen,
2. rationale Funktionen von $\varkappa^2$,
3. die drei Funktionen $\operatorname{sn} v$, $\operatorname{cn} v$, $\operatorname{dn} v$,
4. die Größen $\operatorname{sn}\left(\frac{4\mu K' + 4\mu' i K'}{n}\right)$.

Aus (2) folgt dann, daß auch

$$\operatorname{cn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right), \qquad \operatorname{dn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

zum Rationalitätsbereich gehören.

Wir bemerken nun, daß nach dem Additionstheorem jede der Größen $x_{\mu,\mu'}$ durch jede andere unter ihnen rational ausdrückbar ist. Wenn insbesondere

(5) $$x_{\mu,\mu'} = F_{\mu,\mu'}(x_{0,0})$$

ist, so ist

(6) $$x_{\mu+\nu,\mu'+\nu'} = F_{\mu,\mu'}(x_{\nu,\nu'}) = F_{\mu+\nu,\mu'+\nu'}(x_{0,0}).$$

Daraus folgt, daß die Galoissche Gruppe unserer Gleichung aus den n^2 Vertauschungen $S_{\nu,\nu'}$ besteht, die man erhält, wenn man in den Wurzeln $x_{\mu,\mu'}$ die Indizes μ, μ' alle um dasselbe Zahlenpaar ν, ν' vermehrt (wobei jeder Index nach dem Modul n zu nehmen ist).

Denn nach (5) kann jede rationale Funktion der Wurzeln $x_{\mu,\mu'}$ rational durch $x_{0,0}$ in der Form

$$\Phi(x_{0,0})$$

ausgedrückt werden und geht also nach (6) durch die Substitution $S_{\nu,\nu'}$ in $\Phi(x_{\nu,\nu'})$ über; bleibt sie also durch diese Substitution ungeändert, so ist sie rational. Umgekehrt folgt aus der Irreduzibilität, daß jede rationale Gleichung zwischen den Wurzeln, da sie in die Form gesetzt werden kann:

$$\psi(x_{0,0}) = 0,$$

und also

$$\psi(x_{\nu,\nu'}) = 0$$

zur Folge hat, die Substitution $S_{\nu,\nu'}$ gestattet. Die Gruppe der $S_{\nu,\nu'}$ ist aber wegen

$$S_{\nu,\nu'} S_{\mu,\mu'} = S_{\nu+\mu,\nu'+\mu'}$$

eine Abelsche, welche nach der Formel

$$S_{\nu,\nu'} = S_{1,0}^{\nu} S_{0,1}^{\nu'}$$

durch die Basis $S_{1,0}$, $S_{0,1}$ darstellbar ist, und also ist die allgemeine Teilungsgleichung eine Abelsche Gleichung und mithin algebraisch lösbar (Bd. I, § 169f.).

§ 61. Die Teilung der Perioden.

Die weiter noch zu lösende Aufgabe besteht nun darin, auf algebraischem Wege die Größen

(1) $$x_{\mu,\mu'} = \operatorname{sn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

zu bestimmen. Man erhält alle Werte dieser Größe, wenn man μ, μ', voneinander unabhängig, je ein vollständiges Restsystem nach dem Modul n durchlaufen läßt. Diese Werte sind aber auch alle voneinander verschieden, denn $\operatorname{sn} v$ kann nur dann $= \operatorname{sn} v'$ sein, wenn v' kongruent v oder kongruent $2K - v$ modulo $4K$, $2iK'$, und beides kann für zwei verschiedene der Argumente von (1) nicht eintreten.

Die n^2 Größen (1) sind die Wurzeln der Gleichung

(2) $$x A(x^2) = 0,$$

und nach den Formeln

(3) $$y = \frac{D(x^2)}{B(x^2)}, \qquad z = \frac{D(x^2)}{C(x^2)}$$

können auch

$$y_{\mu,\mu'} = \operatorname{cn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right),$$

$$z_{\mu,\mu'} = \operatorname{dn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right)$$

rational durch $x_{\mu,\mu'}$ ausgedrückt werden, wenn der Rationalitätsbereich aus rationalen Zahlen und rationalen Funktionen von $\varkappa^2$ besteht.

Aus den Wurzeln x^2 der Gleichung $A = 0$ lassen sich nach § 60, (2) und § 44, (18), (19), (20) die Wurzeln von $B = 0$, $C = 0$, $D = 0$ rational ableiten; wenn nämlich x^2 eine Wurzel von $A = 0$ ist, so sind

$$\frac{1-x^2}{1-\varkappa^2 x^2}, \qquad \frac{1-\varkappa^2 x^2}{\varkappa^2(1-x^2)}, \qquad \frac{1}{\varkappa^2 x^2}$$

die Wurzeln von $B = 0$, $C = 0$, $D = 0$. Die Bedeutung dieser letzteren Wurzel ist aber

$$\operatorname{sn}\left(\frac{(4\mu+1)K + 4\mu' iK'}{n}\right)^2,$$

$$\operatorname{sn}\left(\frac{(4\mu+1)K + (4\mu'+1)iK'}{n}\right)^2,$$

$$\operatorname{sn}\left(\frac{4\mu K + (4\mu'+1)iK'}{n}\right)^2,$$

und hiernach sind durch Auflösung der Gleichung $A = 0$ alle Größen von der Form

$$\operatorname{sn}\left(\frac{\mu K + \mu' iK'}{n}\right)^2,$$

worin μ, μ' beliebige ganze Zahlen sind, rational bestimmt.

§ 62. Die Abelschen Relationen.

Für eine nähere Untersuchung der algebraischen Natur der Periodenteilungsgleichung ist ein System von Relationen zwischen ihren Wurzeln von großer Wichtigkeit, zu dessen Ableitung wir jetzt übergehen [1]).

Wir betrachten die Summe:

$$(1) \qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(u + \frac{2\nu}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu}{n}\right)},$$

genommen nach ν über ein volles Restsystem für den (ungeraden) Modul n. ν' ist eine beliebige ganze Zahl und g_1, g_2 eine der drei geraden Charakteristiken $(0, 0)$, $(0, 1)$, $(1, 0)$. Diese Summe ist unabhängig von dem besonderen Restsystem, das man für ν genommen hat.

[1]) Diese Relationen rühren von Abel her (Oeuvres complètes, Bd. I, S. 523; Bd. II, S. 251 der neuen Ausgabe). Der oben gegebene Beweis dieser Relationen schließt sich an Hermite an (Crelles Journal, Bd. 32, S. 283). Zu erwähnen ist noch Sylow, Christiania Videnskabsselskabs Forhandlinger 1864 und 1871. Kronecker, Berichte der Berliner Akademie, 19. Juli 1875. Engel, Berichte der Sächsischen Gesellschaft der Wissenschaften, 31. Juli 1884.

Der Hauptnenner der in (1) vorkommenden Brüche:

$$\overset{\nu}{\Pi}\,\vartheta_{g_1, g_2}\left(u + \frac{2\nu}{n}\right) = \pm \overset{\nu}{\Pi}\,\vartheta_{g_1, g_2}\left(u + \frac{\nu}{n}\right)$$

ist nach den letzten Formeln des § 33, von einem konstanten Faktor abgesehen, gleich

$$\vartheta_{g_1, g_2}(nu, n\omega),$$

und wenn wir also die Summe (1) gleich

$$(2) \qquad \frac{\Phi(u)}{\vartheta_{g_1, g_2}(nu, n\omega)}$$

setzen, so ist $\Phi(u)$ eine ganze transzendente Funktion von u. Nun ist

$$\frac{\vartheta_{11}\left(u + \frac{2\nu+1}{u}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu+1}{u}\right)} = (-1)^{g_1+1} \frac{\vartheta_{11}\left(u + \frac{2\nu+n+1}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu+n+1}{n}\right)}$$

und ν durchläuft gleichzeitig mit $\nu + \frac{1}{2}(n+1)$ ein volles Restsystem nach n. Daraus ergibt sich nach (1) und (2)

$$(3) \qquad \Phi\left(u + \frac{1}{n}\right) = -e^{-\frac{4\nu'\pi i}{n}}\,\Phi(u)$$

und ähnlich

$$(4) \qquad \Phi(u + \omega) = -e^{-n\pi i(2u+\omega)}\,\Phi(u).$$

Daraus ergibt sich, daß die Funktion $\Phi(u)$ eine t-Funktion ist mit den Perioden $1/n$, ω, die durch die Bedingungen (3), (4) bis auf einen von u unabhängigen Faktor bestimmt und durch eine ϑ-Funktion ausdrückbar ist (§ 19). Man sieht leicht, daß die Bedingungen (3), (4) durch die Funktion

$$e^{-4\pi i\nu' u}\,\vartheta_{11}(nu - 4\nu'\omega, n\omega)$$

befriedigt sind, so daß sich ergibt:

$$(5) \quad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(u + \frac{2\nu}{n}\right)}{\vartheta_{g_1, g_2}\left(u + \frac{2\nu}{n}\right)} = Ce^{-4\pi i\nu' u}\,\frac{\vartheta_{11}(nu - 2\nu'\omega, n\omega)}{\vartheta_{g_1, g_2}(nu, n\omega)}.$$

Die Bestimmung der Konstanten C kann man leicht ausführen, wenn man rechts und links mit

$$\vartheta_{g_1, g_2}(u)$$

multipliziert und dann

$$u = \frac{(1 - g_2) + (1 - g_1)\omega}{2}$$

setzt. Die Formel (2) des § 21 ergibt dann:

$$(6)\qquad C = (-1)^{(g_1+1)(g_2+1)\frac{n-1}{2}}\, n\, \frac{\vartheta_{g_1,g_2}(0,\omega)}{\vartheta_{g_1,g_2}(2\nu'\omega, n\omega)}\, \frac{\vartheta'_{11}(0, n\omega)}{\vartheta'_{11}(0,\omega)}.$$

Die Abelschen Relationen erhält man einfach, indem man in (5) $nu = 2\nu'\omega$ setzt, wodurch die rechte Seite verschwindet:

$$(7)\qquad \sum^{\nu} e^{\frac{2\nu'\nu' \pi i}{n}} \frac{\vartheta_{11}\left(\frac{2\nu'\omega + 2\nu}{n}\right)}{\vartheta_{g_1,g_2}\left(\frac{2\nu'\omega + 2\nu}{n}\right)} = 0.$$

Wendet man auf die hier vorkommenden ϑ-Funktionen eine lineare Transformation

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \qquad \alpha\delta - \beta\gamma = 1$$

an, so erhält man nach § 39 die allgemeine Formel:

$$(8)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} \frac{\vartheta_{11}\left(\frac{2(\nu\alpha + \nu'\gamma) + 2(\nu\beta + \nu'\delta)\omega}{n}\right)}{\vartheta_{g_1,g_2}\left(\frac{2(\nu\alpha + \nu'\gamma) + 2(\nu\beta + \nu'\delta)\omega}{n}\right)} = 0.$$

Diese Gleichungen gehen nun, wenn man $g_1, g_2 = 0, 1$ setzt und die Bezeichnungen des § 42 einführt, unmittelbar in Relationen zwischen den Wurzeln $x_{\nu,\nu'}$ (§ 61) über:

$$(9)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}}\, x_{\nu\alpha+\nu'\gamma,\, \nu\beta+\nu'\delta} = 0,$$

und den beiden speziellen Fällen:

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \qquad \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$$

entsprechend:

$$(10)\qquad \sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}}\, x_{\nu,\nu'} = 0,$$

$$(11)\qquad \sum^{\nu'} e^{-\frac{8\nu\nu'\pi i}{n}}\, x_{\nu,\nu'} = 0.$$

Nach (5), (6) kann man auch den Wert dieser Summen bestimmen, wenn darin die n^{te} Einheitswurzel

$$e^{\frac{8\pi i}{n}}$$

durch eine andere ersetzt wird, indem man in (5) ν' durch ein anderes Zeichen, m, ersetzt und dann $nu = 2\nu'\omega$ setzt. Beschränken wir uns auf den Fall $(g_1, g_2) = (0, 1)$ und multipliziert (5) noch mit $\vartheta_{00} : \vartheta_{10}$, so folgt:

$$(12) \qquad \sum^{\nu} e^{\frac{8m\nu\pi i}{n}} x_{\nu,\nu'} = (-1)^{\frac{n-1}{2}} n e^{\frac{-4\pi i m\nu'\omega}{n}} \frac{\vartheta_{00}\vartheta_{01}\vartheta'_{11}(0, n\omega)\vartheta_{11}[2(\nu' - m)\omega, n\omega]}{\vartheta_{10}\vartheta'_{11}\vartheta_{01}(2m\omega, n\omega)\vartheta_{01}(2\nu'\omega, n\omega)},$$

wo die linke Seite dann, aber auch nur dann verschwindet, wenn $m \equiv \nu' \pmod{n}$ ist.

§ 63. Die Galoissche Gruppe der Teilungsgleichung.

Im dreizehnten Abschnitt des ersten Bandes ist gezeigt, wie die algebraische Natur einer Gleichung ihren einfachsten Ausdruck in der Galoisschen Gruppe der Gleichung findet.

Es sei hier kurz an die Definition der Galoisschen Gruppe erinnert.

Nachdem der Rationalitätsbereich Ω festgesetzt war, ist die Galoissche Gruppe einer Gleichung $F(x) = 0$, von der nur vorausgesetzt wird, daß sie keine gleichen Wurzeln habe, definiert als die Gruppe G der Permutationen unter den Wurzeln dieser Gleichung, der die doppelte Eigenschaft zukommt:

a) Jede rationale Gleichung in Ω, die zwischen den Wurzeln von $F(x)$ besteht, bleibt richtig, wenn die Wurzeln irgend einer Permutation dieser Gruppe unterworfen werden.

b) Jede rationale Funktion in Ω von den Wurzeln von $F(x)$, die sämtliche Permutationen der Gruppe gestattet, ist in Ω enthalten.

Indem wir nun die Gruppe G der Teilungsgleichung zu bestimmen suchen, setzen wir als Rationalitätsbereich zunächst den Inbegriff aller rationalen Zahlen und rationalen Funktionen von $\varkappa^2$ voraus.

Nach dem Additions- und Multiplikationstheorem (vgl. § 57, 61) ist, wenn f und φ_m rationale Funktionen bedeuten, die von μ, μ' ν, ν' unabhängig sind,

$$(1) \qquad x_{\mu+\nu, \mu'+\nu'} = f(x_{\mu,\mu'}, x_{\nu,\nu'}),$$

$$(2) \qquad x_{m\mu, m\mu'} = \varphi_m(x_{\mu,\mu'}).$$

Ist nun S irgend eine Substitution der Gruppe $\mathfrak{G}$, durch die, wenn a, b, c, ∂ ganze Zahlen bedeuten, die nach dem Modul n genommen sind,

$$x_{1,0},\ x_{0,1} \quad \text{in} \quad x_{\partial,-c},\ x_{-b,a}$$

übergeht, so können wir S auf jede der Formeln (1), (2) anwenden. Es ist aber nach (2):

$$x_{\mu,0} = \varphi_\mu(x_{1,0}),$$

woraus zu schließen, daß durch die Substitution S

$$x_{\mu,0} \quad \text{in} \quad \varphi_\mu(x_{\partial,-c}) = x_{\partial\mu,-c\mu}$$

übergeht. Ebenso findet man, daß durch S

$$x_{0,\mu'} \quad \text{in} \quad \varphi_{\mu'}(x_{-b,a}) = x_{-b\mu',a\mu'}$$

übergeht.

Wenden wir dies auf die aus (1) hervorgehende Gleichung

$$x_{\mu,\mu'} = f(x_{\mu,0}, x_{0,\mu'})$$

an, so folgt, daß durch S

(3) $$x_{\mu,\mu'} \quad \text{in} \quad x_{\partial\mu-b\mu',-c\mu+a\mu'}$$

übergeht.

Hieraus schließen wir zunächst, daß die Zahlen a, b, c, ∂ so beschaffen sein müssen, daß ihre Determinante

(4) $$m = a\partial - bc$$

mit n keinen Teiler gemein hat. Denn wäre ein solcher Teiler vorhanden, so würden μ, μ', ohne daß beide durch n teilbar sind, so bestimmt werden können, daß

$$\partial\mu - b\mu' \equiv 0, \quad -c\mu + a\mu' \equiv 0 \pmod{n},$$

und es würden mehrere voneinander verschiedene Wurzeln $x_{\mu,\mu'}$ durch S in ein und dieselbe Wurzel übergehen, was unmöglich ist. Denn zunächst können weder a und b noch c und ∂ einen Teiler mit n gemein haben, weil sonst, wenn $a\mu', b\mu'$ oder $c\mu, \partial\mu$ durch n teilbar genommen werden, alle $x_{\mu',0}$ oder alle $x_{0,\mu}$ in $x_{0,0}$ übergehen würden. Setzt man dann $m\mu = n(ha + h'b)$, $m\mu' = n(hc + h'\partial)$, und bestimmt h und h' so, daß $ha + h'b$ keine Teiler mit n gemein hat, so brauchen, wenn n und m einen gemeinsamen Teiler haben, μ, μ' nicht beide durch n teilbar zu sein, und es geht nicht nur $x_{0,0}$, sondern auch $x_{\mu,\mu'}$ nach (3) in $x_{0,0}$ über.

Bezeichnen wir abgekürzt die Vertauschung (3) mit

$$(x_{\mu,\mu'},\ x_{\nu,\nu'}),$$

so ist

$$\begin{aligned} \nu &\equiv \partial\mu - b\mu' \\ \nu' &\equiv -c\mu + a\mu' \end{aligned} \pmod{n},$$

und daraus, durch Auflösung, mit Benutzung der Bezeichnung § 28, (4):

(5) $$m(\mu, \mu') \equiv \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} (\nu, \nu').$$

Es ist daher

(6) $$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

ein zweckmäßiges Zeichen für die Vertauschung S, und aus (5) ersieht man, daß sich zwei solche Vertauschungen:

$$S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \qquad S' = \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix}$$

genau nach der in § 28 gegebenen Regel:

(7) $$SS' = S'' = \begin{pmatrix} aa' + bc', & ab' + b\partial' \\ ca' + \partial c', & cb' + \partial\partial' \end{pmatrix}$$

zusammensetzen, so daß die Vertauschung S'' der Wurzeln entsteht, wenn zuerst die Vertauschung S, sodann die Vertauschung S' unter den Wurzeln der Teilungsgleichung vorgenommen wird. Zu beachten ist aber immer, daß hier nur die nach dem Modul n genommenen Reste der Zahlen a, b, c, ∂ in Betracht kommen, so daß die Anzahl der Vertauschungen S stets endlich ist[1]).

1. Der Inbegriff aller Substitutionen $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ bildet eine Gruppe, die wir mit $\mathfrak{A}$ bezeichnen, und in ihr ist, wie wir bewiesen haben, die Gruppe $\mathfrak{G}$ der Teilungsgleichung enthalten.

In $\mathfrak{A}$ ist als Teiler eine Gruppe $\mathfrak{B}$ enthalten, die aus allen Substitutionen (5)

(8) $$T = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

besteht, die der Bedingung

(9) $$\alpha\delta - \beta\gamma \equiv 1 \pmod{n}$$

genügen.

---

[1]) Wollte man, was auf den ersten Blick näher zu liegen scheint, die Bezeichnung $S = \begin{pmatrix} \partial, & -b \\ -c, & a \end{pmatrix}$ wählen, so würde die Komposition nach der Formel $S'S = S''$, also umgekehrt wie bei der üblichen Komposition der Permentationen, zu bezeichnen sein.

Jede Substitution S läßt sich durch Zusammensetzung von

$$\begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix}$$

mit einer Substitution T herleiten; man hat, damit

$$S = \begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix} T$$

sei, $\alpha, \beta, \gamma, \delta$ einfach aus den Kongruenzen

$$a \equiv \alpha m, \quad b \equiv \beta m, \quad c \equiv \gamma, \quad d \equiv \delta \pmod{n}$$

zu bestimmen.

Wir betrachten nun

$$(10) \qquad x_{\mu,\mu'} = \operatorname{sn}\left(\frac{4\mu K + 4\mu' i K'}{n}\right) = \frac{\vartheta_{00}\vartheta_{11}\left(\frac{2\mu + 2\mu'\omega}{n}\right)}{\vartheta_{10}\vartheta_{01}\left(\frac{2\mu + 2\mu'\omega}{n}\right)},$$

$$\varkappa^2 = \frac{\vartheta_{10}^4}{\vartheta_{00}^4}$$

als Funktionen von ω, und wenden darauf eine lineare Transformation

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \equiv \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix} \pmod{8}$$

an, indem wir ω durch

$$(11) \qquad \omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

ersetzen; dann ergibt sich nach den Formeln (3), (5) und (6), § 39, daß

$$x_{\mu,\mu'} \text{ in } x_{\alpha\mu + \gamma\mu', \beta\mu + \delta\mu'}$$

übergeht, d. h. es erleiden die $x_{\mu,\mu'}$ eine Substitution, die nach (3), (6) mit

$$T = \begin{pmatrix} \delta, & -\gamma \\ -\beta, & \alpha \end{pmatrix}$$

zu bezeichnen ist, während $\varkappa^2$ ungeändert bleibt.

Auf diese Weise kann auch umgekehrt jede der Substitutionen T entstehen; denn wenn irgend eine Substitution T gegeben ist, so kann man durch Hinzufügen passender Vielfachen der (ungeraden) Zahl n zu den Zahlen $\alpha, \beta, \gamma, \delta$ den Bedingungen

$$\alpha \equiv 1, \quad \delta \equiv 1, \quad \beta \equiv 0, \quad \gamma \equiv 0 \pmod{8}$$

immer genügen.

Irgend eine rationale Gleichung zwischen den Wurzeln $x_{\mu,\mu'}$ und $\varkappa^2$ geht, auch wenn beliebige konstante, d. h. von ω unabhängige Zahlenkoeffizienten darin vorkommen, durch (10) in eine Identität über, und man kann daher für ω

$$\frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

substituieren, d. h. man kann jede Substitution T auf die rationale Gleichung zwischen den $x_{\mu,\mu'}$ anwenden. Daraus folgt, daß die ganze Gruppe $\mathfrak{B}$ in $\mathfrak{G}$ enthalten ist (Bd. I, § 156) und sogar in der Gruppe $\mathfrak{G}'$, die aus der Gruppe $\mathfrak{G}$ der Teilungsgleichung durch Adjunktion beliebiger Zahlen entsteht.

Wenn wir den Rationalitätsbereich der rationalen Zahlen durch Adjunktion von $n$ten Einheitswurzeln erweitern, so gehören zu den rationalen Gleichungen auch die Abelschen Relationen des vorigen Paragraphen. Auf diese Relationen, etwa auf

$$\sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu,\nu'} = 0$$

ist aber keine der Substitutionen

$$M = \begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix},$$

in der m von 1 verschwindet, anwendbar; denn durch diese Substitution geht, wenn $mm' \equiv 1 \pmod{n}$ ist,

$$\sum^{\nu} e^{\frac{8\nu\nu'\pi i}{n}} x_{\nu,\nu'} \text{ in } \sum^{\nu} e^{\frac{8\nu m'\nu'\pi i}{n}} x_{\nu,\nu'}$$

über, was nach (12), § 62 von Null verschieden ist, wenn nicht m' und also auch $m \equiv 1 \pmod{n}$ ist. Daraus folgt der Satz:

2. Nach Adjunktion der $n$ten Einheitswurzeln (und beliebiger anderer Konstanten) ist $\mathfrak{B}$ die Galoissche Gruppe der Teilungsgleichung. Es wird $\mathfrak{B}$ auch die Monodromiegruppe der Teilungsgleichung genannt.

3. Wir beweisen jetzt noch, daß in dem ursprünglichen Rationalitätsbereich, also ohne Adjunktion der $n$ten Einheitswurzeln oder anderer irrationaler Zahlen, die Gruppe der Teilungsgleichung mit der Gruppe $\mathfrak{A}$ identisch ist.

Es ist in Bd. I, § 174 gezeigt, daß die primitiven $n$ten Einheitswurzeln ϱ Wurzeln einer irreduziblen Gleichung

(12) $$\Phi(\varrho) = 0$$

sind, und diese Gleichung kann auch nicht zerfallen, wenn der unabhängigen Veränderlichen $\varkappa^2$ durch Adjunktion der Rationalitätsbereich der rationalen Zahlen erweitert wird.

Der Grad dieser Gleichung ist $\varphi(n)$, d. h. gleich der Anzahl der Modulo n inkongruenten Zahlen m, die relativ prim zu n sind.

Es sei nun

$$F(r) = 0 \tag{13}$$

eine Galoissche Resolvente vom Grade μ der Teilungsgleichung im ursprünglichen Rationalitätsbereich (so daß alle Wurzeln $x_{\nu,\nu'}$ rational durch r darstellbar sind, Bd. I, § 152). Diese Gleichung muß nach Adjunktion einer Wurzel von (12) zerfallen; denn wäre dies nicht, so würde jede rationale Relation

$$\psi(r, \varrho) = 0 \tag{14}$$

für alle Wurzeln von (13) befriedigt sein, und $\psi(t, \varrho)$ wäre durch $F(t)$ (für ein variables t) teilbar. Es würde also (14) noch bestehen bleiben, wenn ϱ durch eine andere Wurzel ϱ^m von (12) ersetzt wird. Dies ist aber nach § 62, (12) nicht zutreffend, wenn man an Stelle von (14) eine der Abelschen Relationen setzt.

Es sei nun nach Adjunktion von ϱ

$$F(r, \varrho) = 0 \tag{15}$$

die Galoissche Resolvente vom Grade ν der Teilungsgleichung, so daß ν nach 2. gleich dem Grade der Gruppe $\mathfrak{B}$ ist. Es ist dann $F(t)$ durch $F(t, \varrho)$ algebraisch teilbar und also wegen der Irreduzibilität von (12) auch durch jede der Funktionen $F(t, \varrho^m)$. Da die Funktionen $F(t, \varrho^m)$ irreduzibel sind, so können nur dann zwei von ihnen einen gemeinsamen Teiler haben, wenn sie ganz identisch sind. Wenn aber

$$F(t, \varrho) = F(t, \varrho^m)$$

wäre, dann würde aus jeder Gleichung der Form (14) folgen, daß $\psi(t, \varrho)$ durch $F(t, \varrho) = F(t, \varrho^m)$ teilbar wäre, und es würde folgen, daß in (14) die Vertauschung (ϱ, ϱ^m) gestattet ist, was wieder bei den Abelschen Relationen nicht zutrifft. Mithin sind die $\varphi(n)$ Funktionen $F(t, \varrho^m)$ alle voneinander verschieden, und $F(t)$ ist durch ihr Produkt teilbar. Der Grad μ von $F(t)$ ist also wenigstens $= \nu\,\varphi(n)$. Er kann aber auch nicht höher als $\nu\,\varphi(n)$ sein, da $\nu\,\varphi(n)$ der Grad der Gruppe $\mathfrak{A}$ ist, und die

Gruppe 𝔊 vom Grade μ gewiß in 𝔄 enthalten ist. Es ergibt sich hieraus

(16) $$\mu = \nu\,\varphi(n)$$

und zugleich die Identität von 𝔊 mit 𝔄.

Daraus folgt aber auch, daß $F(t)$ dem Produkt der sämtlichen Faktoren $F(t, \varrho^m)$ gleich ist, also

(17) $$F(t) = \overset{m}{\Pi} F(t, \varrho^m),$$

und da $F(t) = 0$ keine gleichen Wurzeln hat, daß zwar $F(r, \varrho)$, aber keiner von den anderen Faktoren $F(r, \varrho^m)$ verschwindet. Die Gleichungen

(18) $$F(r, t) = 0, \quad \Phi(t) = 0$$

haben daher nur die eine Wurzel $t = \varrho$ miteinander gemein, und durch Aufsuchen ihres größten gemeinschaftlichen Teilers findet man ϱ rational ausgedrückt durch r, d. h. durch die Wurzeln der Teilungsgleichung.

Diese Ausdrücke für ϱ ändern ihren Wert nicht, wenn auf r eine Substitution der Gruppe 𝔅 angewandt wird, während [nach (12)] ϱ durch eine Substitution der Gruppe 𝔄 in eine Potenz von ϱ übergeht.

Die Abelschen Relationen zeigen, daß durch die in 𝔄 enthaltene Substitution

(19) $$\begin{pmatrix} m, & 0 \\ 0, & 1 \end{pmatrix}$$

ϱ in ϱ^m übergeht; denn setzen wir

$$e^{\frac{8\pi i}{n}} = \varrho^\lambda,$$

so lautet eine der Abelschen Relationen

(20) $$\overset{\nu}{\Sigma}\, \varrho^{\lambda\nu\nu'} x_{\nu,\nu'} = 0,$$

worauf, wenn für ϱ der Ausdruck durch r gesetzt wird, alle Substitutionen von 𝔄, also auch (19), anwendbar sind. Nach § 62, (12) bleibt aber (20) bei dieser Substitution nur richtig, wenn ϱ in ϱ^m übergeht.

Da ϱ durch die Substitutionen in 𝔅 nicht geändert wird, und da die Gruppe 𝔄 aus 𝔅 durch Zusammensetzung mit (19) entsteht, so folgt, daß durch irgend eine Substitution in 𝔄

$$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

ϱ in ϱ^m übergeht, wenn m der Determinante $(a\partial - bc)$ nach dem Modul n kongruent ist.

4. Wir wollen schließlich noch die Zahl ν, d. h. den Grad der Gruppe $\mathfrak{B}$ bestimmen.

$\varphi(n)$ hat, wie bekannt, den Ausdruck (Bd. I, § 140)

$$\varphi(n) = n\Pi\left(1 - \frac{1}{p}\right), \tag{21}$$

wenn das Produktzeichen Π sich auf alle in n aufgehenden, voneinander verschiedenen Primzahlen p erstreckt.

Die Zahl ν ist gleich der Anzahl der nach n inkongruenten Zahlensysteme $\alpha, \beta, \gamma, \delta$, die der Bedingung

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{n} \tag{22}$$

genügen. Wir fragen zunächst nach der Anzahl der Paare α, β, lie mit n keinen gemeinschaftlichen Teiler haben, und bezeichnen liese mit $\chi(n)$.

Ist $n = n'n''$ und n' relativ prim zu n'', so kann man aus eder Kombination eines zu n' gehörigen Zahlenpaares α', β' mit inem zu n'' gehörigen Zahlenpaar α'', β'' ein zu n gehöriges

$$\alpha = n''\alpha' + n'\alpha'', \qquad \beta = n''\beta' + n'\beta''$$

erleiten, und man erhält auf diese Weise alle Zahlenpaare α, β ind jedes nur einmal. Daraus folgt:

$$\chi(n) = \chi(n')\chi(n''). \tag{23}$$

Es ist also noch $\chi(p^\pi)$, d. h. $\chi(n)$ für eine Primzahlpotenz $= p^\pi$ zu bestimmen.

Setzen wir zunächst für α, β alle modulo p^π verschiedenen ahlen, so ist diese Anzahl $p^{2\pi}$. Hiervon sind aber alle die aare wegzulassen, bei denen α und β durch p teilbar sind, eren Anzahl $p^{2\pi-2}$ beträgt, so daß

$$\chi(p^\pi) = p^{2\pi} - p^{2\pi-2},$$

nd folglich nach (23) allgemein

$$\chi(n) = n^2\Pi\left(1 - \frac{1}{p^2}\right) \tag{24}$$

lgt, wenn p die in n aufgehenden Primzahlen durchläuft.

Jedes Zahlenpaar α, β läßt sich durch Vermehrung um Vielche von n in ein solches verwandeln, deren Zahlen unter sich lativ prim sind, und dann läßt sich γ, δ so bestimmen, daß

$$\alpha\delta - \beta\gamma = 1$$

wird, darin kann γ, δ durch $\gamma + h\alpha$, $\delta + h\beta$ ersetzt werde: und indem man h ein volles Restsystem modulo n durchlaufe läßt, erkennt man, daß zu jedem Zahlenpaar α, β n der Bedingun (23) genügende Zahlenpaare γ, δ gehören. Demnach ist die Orc nung der Gruppe 𝔅:

$$\nu = n^3 \Pi\left(1 - \frac{1}{p^2}\right),$$

oder, wenn wir noch die numerische Funktion

$$\psi(n) = n\Pi\left(1 + \frac{1}{p}\right) \tag{25}$$

einführen:

$$\nu = n\varphi(n)\psi(n) \tag{26}$$

und die Ordnung der Gruppe 𝔄:

$$\mu = n\varphi(n)^2\psi(n). \tag{27}$$

§ 64. Die irreduzibeln Faktoren der Teilungsgleichung.

Ist

$$\begin{aligned} \nu &= \quad \partial\mu - b\mu' \\ \nu' &= -c\mu + a\mu' \end{aligned}$$

und $a\partial - bc$ relativ prim zu n, so ist der größte gemeinschaft liche Teiler von μ, μ', n zugleich der größte gemeinschaftlich Teiler von ν, ν', n. Die Wurzeln $x_{\mu,\mu'}$ der Teilungsgleichun zerfallen also nach dem größten gemeinschaftlichen Teiler vo μ, μ', n in Systeme, die durch die Substitutionen der Gruppe 𝔄 immer nur ineinander übergehen, d. h. die Gruppe 𝔊 ist in transitiv, und die Systeme der Intransitivität sind di Systeme $x_{\mu,\mu'}$, in denen μ, μ', n einen und denselben größte gemeinschaftlichen Teiler haben. Die Teilungsgleichung ist als reduzibel (außer wenn n eine Primzahl ist) und die Wurzeln eines dieser Systeme der Imprimitivität genügen einer rationale Gleichung (Bd. I, § 157).

Nach dem vorhergehenden Paragraphen gibt es $\varphi(n)\psi(n)$ Zahlenpaare μ, μ', deren größter gemeinschaftlicher Teiler mit n gleich 1 ist, und die diesen Zahlenpaaren entsprechenden Wurzeln $x_{\mu,\mu'}$ genügen daher einer rationalen Gleichung des Grades $\varphi(n)\psi(n)$ Diese Gleichung nennen wir die eigentliche Teilungsgleichung für den Divisor n, weil nur dann, wenn μ, μ', n ohne gemeinsamen Teiler sind, $x_{\mu,\mu'}$ nicht zugleich Wurzel einer Teilungs-

gleichung für einen kleineren Divisor ist. Im Gegensatz hierzu nennen wir die Gleichung, deren Wurzeln die sämtichen $x_{\mu,\mu'}$ sind, die allgemeine Teilungsgleichung für den Divisor n.

Durch irgend eine Substitution der Gruppe $\mathfrak{A}$

$$S = \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

geht $(1,0)$, $(0,1)$ in $(\partial, -c)$, $(-b, a)$ über, und wenn also S nicht die identische Substitution ist, so wird gewiß wenigstens eine der beiden Wurzeln $x_{1,0}$, $x_{0,1}$ durch S verändert. Daraus ergibt sich, daß die Galoissche Gruppe der eigentlichen Teilungsgleichung genau dieselbe ist, wie die der allgemeinen, nur angewandt auf den Fall, daß μ, μ', n keinen gemeinsamen Teiler haben, nämlich, je nachdem die $n$ten Einheitswurzeln adjungiert sind oder nicht, $\mathfrak{B}$ oder $\mathfrak{A}$.

Daraus folgt noch, daß die eigentliche Teilungsgleichung irreduzibel ist, selbst nach Adjunktion beliebiger Konstanten.

Denn sind γ, δ irgend zwei Zahlen ohne gemeinsamen Teiler mit n, so kann man α, β der Kongruenz

$$\alpha\delta - \beta\gamma \equiv 1 \pmod{n}$$

gemäß bestimmen und die in $\mathfrak{B}$ enthaltene Substitution

$$T = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

auf jede rationale Gleichung zwischen den Wurzeln $x_{\mu,\mu'}$ anwenden. Wenn also $x_{1,0}$ einer rationalen Gleichung (mit beliebigen konstanten Koeffizienten)

$$\Phi(x_{1,0}) = 0$$

genügt, so genügt derselben Gleichung jede andere Wurzel $x_{\delta,-\gamma}$ der eigentlichen Teilungsgleichung, woraus die Irreduzibilität der letzteren folgt.

§ 65. Zurückführung der Teilungsgleichung auf Transformationsgleichungen.

Die Wurzeln der eigentlichen Teilungsgleichung lassen sich in folgender Weise in Reihen anordnen. Man wähle nach Belieben eine der Wurzeln:

$$x_{\mu_1,\mu'_1} = \operatorname{sn}\left(\frac{4\mu_1 K + 4\mu'_1 iK'}{n}\right) = \operatorname{sn}\Omega_1.$$

Unter den Wurzeln der Teilungsgleichung kommen auch die $\varphi(n)$ Größen

$$(R_1) \qquad \operatorname{sn} h\,\Omega_1$$

vor, die, wenn h ein vollständiges System inkongruenter zu n teilerfremder Zahlen durchläuft, alle voneinander verschieden sind. Das System (R_1) wollen wir die erste Reihe der Wurzeln nennen.

Ist nun $\operatorname{sn}\Omega_2$ eine in (R_1) nicht enthaltene Wurzel, so bilden die $\varphi(n)$ Größen

$$(R_2) \qquad \operatorname{sn} h\,\Omega_2,$$

die sowohl untereinander als von den Wurzeln (R_1) verschieden sind, eine zweite Reihe; und auf diese Weise kann man fortfahren, bis sämtliche $\varphi(n)\,\psi(n)$ Wurzeln der eigentlichen Teilungsgleichung in $\psi(n)$ Reihen von je $\varphi(n)$ Gliedern verteilt sind.

Nach dem Multiplikationstheorem läßt sich durch eine Wurzel jede andere Wurzel derselben Reihe rational ausdrücken in der Form:

$$(1) \qquad \operatorname{sn} h\,\Omega = f_h(\operatorname{sn}\Omega),$$

worin f_h eine nur von dem Multiplikator h, nicht von der Wahl von Ω abhängige rationale Funktion ist.

Wenn die beiden Wurzeln $x_{\mu,\mu'}$, $x_{\nu,\nu'}$ in dieselbe Reihe gehören, so muß sich die Zahl h so bestimmen lassen, daß

$$(2) \qquad h\,\mu \equiv \nu, \quad h\,\mu' \equiv \nu' \pmod{n},$$

und umgekehrt, wenn dies der Fall ist, so gehören die beiden Wurzeln in dieselbe Reihe. Aus (2) aber folgt die Kongruenz

$$(3) \qquad \mu\,\nu' - \nu\,\mu' \equiv 0 \pmod{n},$$

und aus dieser lassen sich auch umgekehrt die Kongruenzen (2) wieder herleiten.

Denn da μ, μ', n relativ prim sind, so kann man die Zahlen α, β so bestimmen, daß

$$\alpha\,\mu - \beta\,\mu' \equiv 1 \pmod{n}$$

wird, und daraus folgt mittels (3):

$$\nu \equiv (\alpha\,\nu - \beta\,\nu')\,\mu, \quad \nu' \equiv (\alpha\,\nu - \beta\,\nu')\,\mu' \pmod{n},$$

also, wenn $\alpha\,\nu - \beta\,\nu' = h$ gesetzt wird, die Kongruenzen (2).

Die Kongruenz (3) ist also die notwendige und hinreichende Bedingung dafür, daß die beiden Wurzeln der eigentlichen Teilungsgleichung $x_{\mu,\mu'}$, $x_{\nu,\nu'}$ derselben Reihe angehören.

Hieraus folgt, daß die Einteilung in Reihen gänzlich unabhängig ist von der Willkürlichkeit in der Annahme über die Wurzeln $\operatorname{sn} \Omega_1$, $\operatorname{sn} \Omega_2$ ...

Es folgt aber noch weiter daraus, daß durch die Substitutionen der Gruppe $\mathfrak{A}$ die Reihen nicht auseinandergerissen, sondern nur untereinander vertauscht werden. Die Gruppe der Teilungsgleichung ist also imprimitiv, und die einzelnen Reihen sind die Systeme der Imprimitivität (Bd. I, § 158).

Denn wendet man auf (μ, μ') und (ν, ν') gleichzeitig die Substitution

$$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

an, so bleibt die Kongruenz (3) erhalten.

Sucht man unter den Substitutionen der Gruppe $\mathfrak{A}$ die Substitutionen aus, welche die Wurzeln einer Reihe nur untereinander vertauschen, so erhält man eine Gruppe, und zwar einen Teiler von $\mathfrak{A}$. Zu jeder Reihe gehört also ein solcher Teiler von $\mathfrak{A}$. Bezeichnen wir mit $R_{\mu,\mu'}$ die Reihe, in der die Wurzel $x_{\mu,\mu'}$ vorkommt, und mit $\mathfrak{A}_{\mu,\mu'}$ den zu dieser Reihe gehörigen Divisor von $\mathfrak{A}$, so sind nach (3) [vgl. § 63, (3)] die Substitutionen

$$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

von $\mathfrak{A}_{\mu,\mu'}$ durch die Kongruenz

(4) $$(\partial \mu - b \mu') \mu' + (c \mu - a \mu') \mu \equiv 0 \pmod{n}$$

charakterisiert.

Ebenso erhält man eine Gruppe $\mathfrak{B}_{\mu,\mu'}$, wenn man die Substitutionen in $\mathfrak{B}$ aufsucht, die die Wurzeln der Reihe $R_{\mu,\mu'}$ nur unter sich vertauschen, deren Substitutionen:

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

durch die beiden Kongruenzen:

(5) $$\left.\begin{aligned} (\delta \mu - \beta \mu') \mu' + (\gamma \mu - \alpha \mu') \mu &\equiv 0 \\ \alpha \delta - \beta \gamma &\equiv 1 \end{aligned}\right. \pmod{n}$$

charakterisiert sind.

Beispielsweise bestehen die Gruppen $\mathfrak{A}_{1,0}$, $\mathfrak{B}_{1,0}$ aus den Substitutionen

$$\begin{pmatrix} a, & b \\ 0, & \partial \end{pmatrix}, \quad \begin{pmatrix} \alpha, & \beta \\ 0, & \delta \end{pmatrix}, \quad \alpha \delta \equiv 1 \pmod{n}.$$

Die Gruppen $\mathfrak{A}_{\mu,\mu'}$ sind konjugierte Divisoren von $\mathfrak{A}$ (Bd. II, § 3), denn wenn $x_{1,0}$ durch S in $x_{\mu,\mu'}$, also $R_{1,0}$ in $R_{\mu,\mu'}$ übergeht, so werden durch die Gruppe

$$S^{-1}\mathfrak{A}_{1,0}S$$

die Wurzeln von $R_{\mu,\mu'}$ nur unter sich vertauscht, und es ist also

(6) $$S^{-1}\mathfrak{A}_{1,0}S = \mathfrak{A}_{\mu,\mu'}.$$

Ebenso ist, wenn T eine Substitution in $\mathfrak{B}$ ist, durch die $x_{1,0}$ in $x_{\mu,\mu'}$ übergeht:

(7) $$T^{-1}\mathfrak{B}_{1,0}T = \mathfrak{B}_{\mu,\mu'}.$$

Der größte gemeinschaftliche Teiler $\mathfrak{A}_0$ aller Gruppen $\mathfrak{A}_{\mu,\mu'}$ wird nach (4) bestimmt durch

$$b \equiv 0, \quad c \equiv 0, \quad a \equiv \partial \pmod{n}$$

und besteht also aus den Substitutionen:

$$\begin{pmatrix} a, & 0 \\ 0, & a \end{pmatrix},$$

worin a eine beliebige, zu n teilerfremde Zahl ist. $\mathfrak{A}_0$ ist identisch mit dem größten gemeinschaftlichen Teiler dreier der Gruppen $\mathfrak{A}_{\mu,\mu'}$, die verschiedenen Reihen angehören. Denn $\mathfrak{A}_0$ ist dann der größte gemeinschaftliche Teiler von $\mathfrak{A}_{\mu,\mu'}$, $\mathfrak{A}_{\nu,\nu'}$, $\mathfrak{A}_{\varrho,\varrho'}$, wenn die drei Kongruenzen

$$\begin{aligned} c\mu^2 - (\partial - a)\mu\mu' - b\mu'^2 &\equiv 0 \\ c\nu^2 - (\partial - a)\nu\nu' - b\nu'^2 &\equiv 0 \pmod{n} \\ c\varrho^2 - (\partial - a)\varrho\varrho' - b\varrho'^2 &\equiv 0 \end{aligned}$$

nur unter der Voraussetzung

$$\partial \equiv a, \quad b \equiv 0, \quad c \equiv 0 \pmod{n}$$

erfüllt sind. Dies findet statt, wenn die Determinante

$$\begin{vmatrix} \mu^2, & \mu\mu', & \mu'^2 \\ \nu^2, & \nu\nu', & \nu'^2 \\ \varrho^2, & \varrho\varrho', & \varrho'^2 \end{vmatrix} = -(\nu\varrho' - \varrho\nu')(\varrho\mu' - \mu\varrho')(\mu\nu' - \nu\mu')$$

relativ prim zu n ist.

Ebenso ist nach (5) der größte gemeinschaftliche Teiler $\mathfrak{B}_0$ aller $\mathfrak{B}_{\mu,\mu'}$ der Inbegriff der Substitutionen:

(8) $$\begin{pmatrix} \alpha, & 0 \\ 0, & \alpha \end{pmatrix}$$

mit der Bedingung:

(9) $$\alpha^2 \equiv 1 \pmod{n}.$$

Die Kongruenz (9) besitzt, wenn k die Anzahl der in n aufgehenden, voneinander verschiedenen Primzahlen ist, 2^k inkongruente Lösungen, und dies ist also der Grad der Gruppe $\mathfrak{B}_0$ [1]).

Eine rationale Funktion ξ der Wurzeln einer Reihe, etwa der Reihe $R_{1,0}$, läßt sich nach (1) rational durch eine dieser Wurzeln darstellen. Wenn diese Funktion die Eigenschaft hat, ungeändert zu bleiben, falls diese eine Wurzel durch eine andere derselben Reihe ersetzt wird, wenn also beispielsweise ξ eine symmetrische Funktion der Wurzeln einer Reihe ist, dann erhält ξ durch Anwendung der Substitutionen von $\mathfrak{A}$ (oder auch von $\mathfrak{B}$) nur

(10) $$\nu = \psi(n)$$

verschiedene Werte

(11) $$\xi_1, \xi_2, \ldots, \xi_\nu,$$

und wenn diese Werte alle voneinander verschieden sind, so gehört ξ zu der Gruppe $\mathfrak{A}_{1,0}$ und alle anderen symmetrischen Funktionen der Wurzeln von $R_{1,0}$ sind rational durch ξ darstellbar (Bd. I, § 162).

Die ν Größen (11) sind die Wurzeln einer irreduzibeln rationalen Gleichung νten Grades, die wir eine Transformationsgleichung nennen.

Die Transformationsgleichung hat, wenn in ξ nur rationale Zahlkoeffizienten vorkommen, selbst rationale Zahlkoeffizienten. Sie bleibt aber irreduzibel, wenn auch $n$te Einheitswurzeln oder überhaupt irgend welche Konstanten adjungiert werden, wie sich daraus ergibt, daß durch Substitutionen der Gruppe $\mathfrak{B}$ jede Wurzel der Teilungsgleichung in jede andere, also auch jede Reihe in jede andere Reihe übergeführt werden kann.

Durch die Adjunktion einer Wurzel ξ der Transformationsgleichung, etwa der zur Gruppe $\mathfrak{A}_{1,0}$ gehörigen, reduziert sich die Gruppe der Teilungsgleichung auf $\mathfrak{A}_{1,0}$, die letztere Gruppe ist aber nicht mehr transitiv, sondern vertauscht die $\varphi(n)$ Wurzeln $x_{h,0}$, worin h ein vollständiges System inkongruenter, zu n teilerfremder Zahlen durchläuft, untereinander. Die Teilungsgleichung wird also reduzibel und hat einen Faktor $\varphi(n)$ten Grades,

---

[1]) Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl., § 37.

dessen Wurzeln die $x_{h,0}$ sind. Der Einfluß einer Substitution der Gruppe $\mathfrak{A}_{1,0}$

$$\begin{pmatrix} a, & b \\ 0, & \partial \end{pmatrix}$$

auf $x_{h,0}$ besteht darin, daß $x_{h,0}$ in $x_{\partial h,0}$ übergeht, und die Gruppe dieser Gleichung $\varphi(n)$ten Grades besteht daher aus den Vertauschungen

$$(x_{h,0},\ x_{\partial h,0}),$$

worin ∂ jede beliebige zu n teilerfremde Zahl sein kann. Diese Gruppe ist eine Abelsche und daher sind die Wurzeln $x_{h,0}$ nach Adjunktion von ξ algebraisch durch Radikale zu bestimmen.

Wenn wir aber nicht nur eine, sondern sämtliche Wurzeln ξ der Transformationsgleichung adjungieren, oder, was auf dasselbe hinauskommt, die drei zu $R_{1,0}$, $R_{0,1}$, $R_{1,1}$ gehörigen, so reduziert sich die Gruppe der Teilungsgleichung auf $\mathfrak{A}_0$, und wenn wir noch $n$te Einheitswurzeln adjungieren, auf $\mathfrak{B}_0$. Die Gruppe $\mathfrak{B}$ ist eine Abelsche vom Grade 2^k, die nur solche Elemente enthält, deren Grad $= 2$ ist. Infolgedessen ist die Teilungsgleichung durch Quadratwurzeln lösbar.

Um die Form dieser Lösung zu finden, setze man

$$n = p^{\pi} p'^{\pi'} \ldots,$$

worin p, p', ... voneinander verschiedene Primzahlen, π, π', .. positive Exponenten sind. Man bestimme die Zahlen c, c', ... aus den Kongruenzen

$$c \equiv -1 \pmod{p^{\pi}}, \qquad c' \equiv -1 \pmod{p'^{\pi'}} \ldots$$
$$c \equiv +1 \pmod{np^{-\pi}}, \quad c' \equiv +1 \pmod{np'^{-\pi'}} \ldots$$

dann erhält man jede Lösung α der Kongruenz

$$\alpha^2 \equiv 1 \pmod{n},$$

und jede nur einmal, in der Form

$$(12) \qquad \alpha \equiv c^{\varepsilon} c'^{\varepsilon'} \ldots \pmod{n},$$

wenn ε, ε', ... die Werte 0, 1 annehmen.

Ist nun Ω irgend einer der Werte

$$\frac{4\mu K + 4\mu' i K'}{n},$$

also $\operatorname{sn}\Omega$ irgend eine Wurzel der eigentlichen Teilungsgleichung, so hat die auf alle α auszudehnende Summe

$$(13)\qquad \Sigma(\pm 1)^{\varepsilon}(\pm 1)^{\varepsilon'}\ldots \operatorname{sn}\alpha\Omega = \psi(\Omega),$$

worin die k Vorzeichen von ± 1 beliebig gewählt werden können, die Eigenschaft, daß für jedes nach (12) bestimmte α

$$(14)\qquad \psi(\alpha\Omega) = (\pm 1)^{\varepsilon}(\pm 1)^{\varepsilon'}\ldots \psi(\Omega)$$

ist, und das Quadrat von $\psi(\Omega)$ bleibt durch die Substitutionen der Gruppe $\mathfrak{B}_0$ ungeändert, ist also durch $n$te Einheitswurzeln und die Wurzeln einer Transformationsgleichung rational ausdrückbar. $\psi(\Omega)$ ist also die Quadratwurzel $\sqrt{A}$ aus einem solchen Ausdruck A. Die Anzahl der Ausdrücke (13) beträgt aber 2^k, und es ergibt sich durch Addition aller so gebildeter Gleichungen

$$(15)\qquad 2^k \operatorname{sn}\Omega = \Sigma\sqrt{A}.$$

Es ist noch zu bemerken, daß von den Größen ψ, also auch von den A, die Hälfte verschwindet. Denn es ist

$$-1 \equiv c c'\ldots \pmod{n},$$

und wenn man also in (14) $\alpha \equiv -1$ setzt, so folgt:

$$\psi(-\Omega) = (\pm 1)(\pm 1)\ldots \psi(\Omega);$$

andererseits ist aber

$$\psi(-\Omega) = -\psi(\Omega),$$

und folglich verschwindet $\psi(\Omega)$ immer dann, wenn unter den in (14) vorkommenden k Größen ± 1 eine gerade Anzahl von negativen Einheiten enthalten ist.

Die Wurzeln $x_{\mu,\mu'}$ können also linear durch 2^{k-1} Quadratwurzeln ausgedrückt werden.

Wenn n eine Primzahl oder eine Potenz einer Primzahl ist, so sind die Quadrate der Wurzeln der Teilungsgleichung rational durch die Wurzeln der Transformationsgleichung ausdrückbar[1]).

Ist n eine zusammengesetzte Zahl, so läßt sich die Einteilung der Wurzeln $x_{\mu,\mu'}$ in Reihen noch weiter treiben. Ist p eine in

---

[1]) Vgl. über diesen Satz Kronecker, Monatsbericht der Berliner Akademie, 19. Juli 1875. Kronecker macht dort auf ein Versehen aufmerksam, das sich in einer diesen Gegenstand betreffenden Abhandlung von Jacobi (Crelle, Bd. 47 und Bd. 50) findet.

n aufgehende Primzahl, so nehme man zwei Wurzeln $x_{\mu,\mu'}$, $x_{\nu,\nu'}$ in dieselbe oder in verschiedene Reihen auf, je nachdem

$$\mu \nu' - \nu \mu' \equiv 0 \pmod{p}$$

oder nicht; gehören hiernach $x_{\nu,\nu'}$ und $x_{\nu_1,\nu_1'}$ in eine Reihe mit $x_{\mu,\mu'}$, so gehören sie auch untereinander in dieselbe Reihe. Die Anzahl der so gebildeten Reihen ist, wie leicht nachzuweisen, $p+1$ und man erhält auf diese Weise als erste Resolvente der Teilungsgleichung eine zum Divisor p gehörige Transformationsgleichung. Wir werden später auf anderem Wege zeigen, wie die Transformationsgleichungen für zusammengesetzte Divisoren auf solche für Primzahldivisoren zurückgeführt werden können.

Siebenter Abschnitt.

Theorie der Transformationsgleichungen.

§ 66. Bildung von Transformationsgleichungen.

Nachdem nun die Teilungsgleichungen auf Transformationsgleichungen zurückgeführt sind, gehen wir an ein genaueres Studium dieser letzteren Gleichungen.

Wir nehmen n ungerade an, verstehen unter p die in n aufgehenden Primzahlen, setzen

$$\nu = \psi(n) = n\,\Pi\left(1 + \frac{1}{p}\right), \tag{1}$$

und bezeichnen die ν Reihen der Wurzeln der Teilungsgleichung mit $R_1, R_2, \ldots, R_\nu$.

Aus jeder dieser Reihen nehmen wir für

$$\Omega_{\mu,\mu'} = \frac{4\mu K + 4\mu' iK'}{n} \tag{2}$$

einen Repräsentanten $\Omega_1, \Omega_2, \ldots, \Omega_\nu$ und erhalten die $\varphi(n)$ Wurzeln einer Reihe, wenn wir in

$$\operatorname{sn} m\Omega$$

m ein vollständiges System inkongruenter zu n teilerfremder Zahlen durchlaufen lassen.

Die einfachsten Ausdrücke, die als Wurzeln von Transformationsgleichungen eingeführt werden können, sind die Produkte

$$\prod_{1,n-1}^{n} \Phi(\operatorname{sn} h\Omega), \tag{3}$$

wenn Φ eine beliebige rationale Funktion ist, und h die Reihe der Zahlen $1, 2, \ldots, n-1$ durchläuft.

Jede solche Funktion ist rational ausdrückbar durch $\operatorname{sn}\Omega$ und bleibt offenbar ungeändert, wenn Ω durch irgend ein $m\Omega$

ersetzt wird; man hat also nur noch dafür zu sorgen, daß die ν Werte von (3), die den ν Reihen entsprechen, voneinander verschieden sind, um (3) zur Wurzel einer (irreduzibeln) Transformationsgleichung zu machen[1]).

Wir nehmen an, die Funktion $\Phi(x)$ sei entweder eine gerade oder eine ungerade Funktion von x, und machen danach folgende Unterscheidung.

Ist $\Phi(x)$ eine gerade Funktion, so sind unter den Faktoren des Produktes (3) je zwei, nämlich

(4) $$\Phi(\operatorname{sn} h\,\Omega), \quad \Phi[\operatorname{sn}(n-h)\,\Omega]$$

einander gleich. Setzen wir also

(5) $$\Pi(\Omega) = \prod_{1,\frac{n-1}{2}}^{h} \Phi(\operatorname{sn} h\,\Omega),$$

so ist, wenn m eine beliebige zu n teilerfremde Zahl ist,

(6) $$\Pi(m\,\Omega) = \Pi(\Omega)$$

[weil unter den $\frac{1}{2}(n-1)$ Zahlen hm nicht zwei eine durch n teilbare Summe oder Differenz haben, also, vom Vorzeichen abgesehen, die $\operatorname{sn} h\,\Omega$ dieselben sind, wie die $\operatorname{sn} hm\,\Omega$]. Es ist also $\Pi(\Omega)$ die Wurzel einer Transformationsgleichung. Diese Klasse von Transformationsgleichungen nennen wir Modulargleichungen.

Ist $\Phi(x)$ eine ungerade Funktion, so sind die beiden Größen (4) entgegengesetzt und (6) ist nicht mehr allgemein richtig, sondern es ist

(7) $$\Pi(m\,\Omega) = \pm\,\Pi(\Omega).$$

Daher ist, wenigstens im allgemeinen, nicht mehr $\Pi(\Omega)$, sondern erst $\Pi(\Omega)^2$ Wurzel einer Transformationsgleichung. Diese Art von Transformationsgleichungen nennen wir Multiplikatorgleichungen. Um die Fälle kennen zu lernen, in denen $\Pi(\Omega)$ selbst Wurzel einer Transformation ist, muß das Vorzeichen in (7) bestimmt werden.

Dies gelingt auf Grund eines Satzes der Zahlentheorie, der im Bd. I, § 145 abgeleitet ist.

Der Satz lautet:

---

[1]) Ausdrücke wie (3) sind auch dann noch Wurzeln von Transformationsgleichungen, wenn h nur zu n teilerfremde Werte annimmt. Solche Transformationsgleichung hat man bisher noch wenig benutzt. Wir werden weiterhin ein Beispiel kennen lernen.

Sind m, n irgend zwei teilerfremde Zahlen, letztere ungerade, bedeutet ferner μ die Anzahl derjenigen unter den Zahlen

$$m,\ 2m,\ 3m \cdots \frac{n-1}{2}\, m,$$

deren absolut kleinste Reste (mod n) negativ sind, so ist

(8) $$(-1)^{\mu} = \left(\frac{m}{n}\right),$$

worin $\left(\frac{m}{n}\right)$ das Legendre-Jacobische Symbol aus der Theorie der quadratischen Reste ist[1]).

Dieser Satz führt nun unmittelbar zur Bestimmung des Vorzeichens in (7). Denn wenn in (5) die Funktion $\Phi(x)$ ungerade ist, so ändern beim Übergang von Ω zu $m\Omega$ genau μ Faktoren in (5) ihr Vorzeichen und wir schließen

(9) $$\Pi(m\Omega) = \left(\frac{m}{n}\right) \Pi(\Omega).$$

Ist n keine Quadratzahl, so kann man m immer so annehmen, daß $\left(\frac{m}{n}\right) = -1$ ist. Ist nämlich $n = p^{\lambda} n'$, λ ungerade, n' nicht durch p teilbar, β ein quadratischer Nichtrest von p, so braucht man m nur aus den Kongruenzen

$$m \equiv \beta \pmod{p^{\lambda}}, \quad m \equiv 1 \pmod{n'}$$

zu bestimmen, um eine solche Zahl m zu finden. Und dann ist $\Pi(m\Omega) = -\Pi(\Omega)$ und nicht $\Pi(\Omega)$, sondern erst $\Pi(\Omega)^2$ Wurzel einer Transformationsgleichung. Ist aber n eine Quadratzahl, so ist $\Pi(m\Omega) = \Pi(\Omega)$ für jedes m und folglich $\Pi(\Omega)$ selbst Wurzel einer Transformationsgleichung. Es folgt also der Satz:

> Bei ungerader Funktion Φ ist $\Pi(\Omega)^2$, und nur wenn n eine Quadratzahl ist, $\Pi(\Omega)$ selbst, Wurzel einer Transformationsgleichung[2]).

---

1) Vgl. über diesen Satz: Schering und Kronecker im Monatsbericht der Berliner Akademie vom 22. Juni 1876. Schering, Acta mathematica I.

2) Diese Vereinfachung der Multiplikatorgleichung in dem Fall, wo n ein Quadrat ist, hat Joubert entdeckt, aber auf einem von dem unserigen ganz verschiedenen Wege nachgewiesen. „Sur les équations, qui se rencontrent dans la théorie de la transformation des fonctions elliptiques." Paris 1876.

§ 67. Besondere Transformationsgleichungen.

Es sollen nun die Wurzeln der Transformationsgleichungen durch ϑ-Funktionen dargestellt werden. Wir setzen zu diesem Zweck:

$$(1)\qquad \begin{aligned} \Omega &= \frac{4\mu K + 4\mu' i K'}{n}, \quad iK' = K\omega, \\ \varpi &= \frac{\mu + \mu'\omega}{n}, \quad \Omega = 4K\varpi \end{aligned}$$

und betrachten die Produkte

$$\prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{01}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{10}(2h\varpi), \quad \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{11}(2h\varpi).$$

Es empfiehlt sich folgende Bezeichnung:

$$(2)\qquad \begin{aligned} P_{00}\vartheta_{00}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}(2h\varpi), \\ P_{10}\vartheta_{10}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{10}(2h\varpi), \\ P_{01}\vartheta_{01}^{\frac{n-1}{2}} &= e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{01}(2h\varpi). \end{aligned}$$

Es ist jetzt die Formel § 39, (9) anzuwenden, die man aber für den gegenwärtigen Zweck etwas anders darstellt.

Setzt man in § 39, (8) $v' = 2h/n$, $v = 2h(\alpha + \beta\omega)/n$ und nimmt abermals das Produkt über $h = 1, 2, \ldots (n-1)/2$, so folgt mit Anwendung von § 32, (24):

$$2^{\frac{n-1}{2}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}\left(\frac{2h(\alpha+\beta\omega)}{n}\right) \vartheta_{01}\left(\frac{2h(\alpha+\beta\omega)}{n}\right) \vartheta_{10}\left(\frac{2h(\alpha+\beta\omega)}{n}\right)$$
$$= (-1)^{\frac{n^2-1}{8}} e^{-\frac{\pi i}{2}\frac{n^2-1}{n}\beta(\alpha+\beta\omega)} \vartheta_{00}^{\frac{n-1}{2}} \vartheta_{10}^{\frac{n-1}{2}} \vartheta_{01}^{\frac{n-1}{2}}\ [1]).$$

Demnach erhält man durch Multiplikation der drei Gleichungen (2):

$$(3)\qquad (-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{00}P_{10}P_{01} = 1.$$

[1]) In § 34, (9) der ersten Auflage ist die betreffende Formel gleich in dieser Form angegeben, die sich auch, wenn auch etwas umständlicher, aus § 39, (9) ableiten läßt.

Außerdem setzen wir noch:

(4) $$P_{11}\eta(\omega)^{\frac{n-1}{2}} = e^{\frac{\pi i}{6}\mu'(\mu+\mu'\omega)\frac{n^2-1}{n}} \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{11}(2h\varpi).$$

Diese Größen P lassen sich durch die Wurzeln der Teilungsgleichung ausdrücken, wenn man unter Anwendung von (3) die Quotienten

$$\frac{P_{00}^2}{P_{01}P_{10}},\quad \frac{P_{10}^2}{P_{01}P_{00}},\quad \frac{P_{01}^2}{P_{10}P_{00}},\quad \frac{P_{11}^3}{P_{00}P_{01}P_{10}}$$

bildet und vermittelst der Formeln des § 42 elliptische Funktionen einführt.

Man erhält so

$$(-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{00}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{dn}^2 h\Omega}{\operatorname{cn} h\Omega},$$

(5) $$(-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{10}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{cn}^2 h\Omega}{\operatorname{dn} h\Omega},$$

$$(-1)^{\frac{n^2-1}{8}} 2^{\frac{n-1}{2}} P_{01}^3 = \prod_{1,\frac{n-1}{2}}^{h} \frac{1}{\operatorname{cn} h\Omega \operatorname{dn} h\Omega},$$

(6) $$(-1)^{\frac{n^2-1}{8}} P_{11}^3 = (\varkappa\varkappa')^{\frac{n-1}{2}} \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn}^3 h\Omega}{\operatorname{cn} h\Omega \operatorname{dn} h\Omega}.$$

Diese Ausdrücke zeigen nun, daß P_{00}^3, P_{10}^3, P_{01}^3 die Wurzeln von Transformationsgleichungen (Modulargleichungen) sind. P_{11}^6 ist die Wurzel einer Multiplikatorgleichung, und wenn n eine Quadratzahl ist, so ist auch P_{11}^3 die Wurzel einer Multiplikatorgleichung.

Man kann in mannigfaltiger Weise die Funktionen P miteinander kombinieren, um neue Transformationsgleichungen zu erhalten. Wir führen folgende an:

(7) $$\frac{P_{10}}{P_{00}} = \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{cn} h\Omega}{\operatorname{dn} h\Omega},\qquad \frac{P_{01}}{P_{00}} = \prod_{1,\frac{n-1}{2}}^{h} \frac{1}{\operatorname{dn} h\Omega},$$

$$(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}} P_{00}^2 P_{11}}{\sqrt{\varkappa \varkappa'}^{\frac{n-1}{3}}} = \prod_{1, \frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega \operatorname{dn} h\Omega}{\operatorname{cn} h\Omega},$$

(8) $$(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}} P_{10}^2 P_{11}}{\sqrt{\varkappa \varkappa'}^{\frac{n-1}{3}}} = \prod_{1, \frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega \operatorname{cn} h\Omega}{\operatorname{dn} h\Omega},$$

$$(-1)^{\frac{n^2-1}{8}} \frac{2^{\frac{n-1}{3}} P_{01}^2 P_{11}}{\sqrt{\varkappa \varkappa'}^{\frac{n-1}{3}}} = \prod_{1, \frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega}{\operatorname{cn} h\Omega \operatorname{dn} h\Omega}.$$

Ein wichtiges Resultat ergibt sich aber noch durch Anwendung des Multiplikationstheorems. Wenn man in der letzten Formel II des § 57 $u = 2h\varpi$ setzt, so findet man

(9) $$e^{4\pi i \omega h^2 \mu'^2} \vartheta_{01}(2h\varpi)^{n^2} = \frac{\vartheta_{01}^{n^2}}{D(\operatorname{sn}^2 h\Omega)},$$

worin, wie wir uns erinnern, D eine ganze rationale Funktion ist, deren Koeffizienten rational aus $\varkappa^2$ und ganzen Zahlen gebildet sind.

Nehmen wir das Produkt aus diesen Ausdrücken, für $h = 1, 2, \ldots, \frac{n-1}{2}$, so folgt aus der letzten Gleichung (2) $\left(\text{weil bekanntlich } \Sigma h^2 = \frac{n(n^2-1)}{24}\right)$:

(10) $$P_{01}^{n^2} = \prod_{1, \frac{n-1}{2}}^{h} \frac{1}{D(\operatorname{sn}^2 h\Omega)}.$$

Wir schließen hieraus, daß auch $P_{01}^{n^2}$ die Wurzel einer Transformationsgleichung ist. Dies ist nichts Neues, wenn n durch 3 teilbar ist, wohl aber, wenn n nicht durch 3, also $n^2 - 1$ durch 3 teilbar ist. Wir erhalten dann nämlich aus (10) mit Benutzung von (5), (7), (8):

$$P_{01} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1, \frac{n-1}{2}}^{h} \frac{(\operatorname{cn} h\Omega)^{\frac{n^2-1}{3}} (\operatorname{dn} h\Omega)^{\frac{n^2-1}{3}}}{D(\operatorname{sn}^2 h\Omega)},$$

(11) $$P_{00} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1, \frac{n-1}{2}}^{h} \frac{(\operatorname{cn} h\Omega)^{\frac{n^2-1}{3}} (\operatorname{dn} h\Omega)^{\frac{n^2+2}{3}}}{D(\operatorname{sn}^2 h\Omega)},$$

$$P_{10} = 2^{\frac{(n-1)(n^2-1)}{6}} \prod_{1, \frac{n-1}{2}}^{h} \frac{(\operatorname{cn} h\Omega)^{\frac{n^2+2}{3}} (\operatorname{dn} h\Omega)^{\frac{n^2-1}{3}}}{D(\operatorname{sn}^2 h\Omega)},$$

$$(12)\qquad (-1)^{\frac{n^2-1}{8}}\, 2^{\frac{n^2(n-1)}{3}}\, P_{11} = \sqrt{\varkappa\varkappa'}^{\frac{n-1}{3}} \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega\, D(\operatorname{sn}^2 h\Omega)^2}{(\operatorname{cn} h\Omega)^{\frac{2n^2+1}{3}} (\operatorname{dn} h\Omega)^{\frac{2n^2+1}{3}}}.$$

Soll als Rationalitätsbereich der der rationalen Zahlen und rationalen Funktionen von $\varkappa^2$ aufrecht erhalten werden, so schreibt man die letzte Gleichung besser in der Form [vgl. § 54, (4)]:

$$(13)\qquad P_{11}\gamma_2(\omega)^{\frac{n-1}{2}} = (-1)^{\frac{n^2-1}{8}}\, 2^{-\frac{(n^2-4)(n-1)}{3}} (\varkappa\varkappa')^{-\frac{n-1}{2}} (1-\varkappa^2\varkappa'^2)^{\frac{n-1}{2}} \times \prod_{1,\frac{n-1}{2}}^{h} \frac{\operatorname{sn} h\Omega\, D(\operatorname{sn}^2 h\Omega)^2}{(\operatorname{cn} h\Omega)^{\frac{2n^2+1}{3}} (\operatorname{dn} h\Omega)^{\frac{2n^2+1}{3}}},$$

und schließt daraus auf den folgenden Satz:

Wenn n nicht durch 3 teilbar ist, so sind P_{00}, P_{01}, P_{10}, $P_{11}^2\gamma_2(\omega)^{n-1}$, und wenn n ein Quadrat ist, auch $P_{11}\gamma_2(\omega)^{\frac{n-1}{2}}$ Wurzeln von Transformationsgleichungen.

§ 68. Zweite Darstellung der Wurzeln der Transformationsgleichungen.

Wenn wir zunächst eine der Reihen ins Auge fassen, nämlich die, zu der die Wurzel $x_{1,0}$ gehört, also $\mu = 1$, $\mu' = 0$ setzen, so können wir auf (2), (3) des vorigen Paragraphen die Formeln (20), (21), (10), § 34 anwenden. Setzt man dort, wenn ν ungerade ist, $n - \nu$ an Stelle von ν und benutzt die Formel

$$\vartheta_{g_1 g_2}\left(\frac{n-\nu}{n}\right) = (-1)^{g_1(g_2+1)}\, \vartheta_{g_1 g_2}\left(\frac{\nu}{n}\right),$$

dann kommen in diesen Formeln nur die geraden ν vor, und wenn man also $\nu = 2h$ setzt, so kann man die dortigen Formeln (20), (21) auch so schreiben:

$$\sqrt{n}\,\eta(n\omega)\,\eta(\omega)^{\frac{n-3}{2}} = \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{11}\left(\frac{2h}{n}\right),$$

$$f(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} = f(\omega) \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{00}\left(\frac{2h}{n}\right),$$

$$f_1(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} = f_1(\omega) \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{01}\left(\frac{2h}{n}\right),$$

$$f_2(n\omega)\,\eta(\omega)^{\frac{n-1}{2}} = \left(\frac{2}{n}\right) f_2(\omega) \prod_{1,\frac{n-1}{2}}^{h} \vartheta_{10}\left(\frac{2h}{n}\right),$$

worin $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$, und wenn wir also die dem Falle $\mu = 1$, $\mu' = 0$ entsprechenden Funktionen P mit P^0 bezeichnen, so folgt aus § 67, (2) und (4) mit Rücksicht auf § 34, (10):

$$P^0_{00} = \frac{f(n\omega)}{f(\omega)^n},$$

$$(1) \qquad P^0_{01} = \frac{f_1(n\omega)}{f_1(\omega)^n},$$

$$P^0_{10} = \left(\frac{2}{n}\right)\frac{f_2(n\omega)}{f_2(\omega)^n},$$

$$(2) \qquad P^0_{11} = \sqrt{n}\,\frac{\eta(n\omega)}{\eta(\omega)}.$$

Um durch solche Formeln die sämtlichen Wurzeln der Transformationsgleichungen darzustellen, bestimmen wir eine lineare Transformation folgendermaßen:

$$(3) \qquad \begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix} \equiv \begin{pmatrix}1, 0\\ 0, 1\end{pmatrix} \pmod{16},$$

$$(4) \qquad \alpha \equiv \mu, \qquad \beta \equiv \mu' \pmod{n},$$

und ersetzen ω in (1), (2) durch

$$(5) \qquad \omega' = \frac{\gamma + \delta\omega}{\alpha + \beta\omega};$$

auf die linke Seite lassen sich dann die Formeln (3) bis (6) § 39 und (19), § 38 anwenden und ergeben:

$$(6) \qquad \begin{aligned} P_{00} &= \frac{f(n\omega')}{f(\omega')^n}, \\ P_{01} &= \frac{f_1(n\omega')}{f_1(\omega')^n}, \\ P_{10} &= \left(\frac{2}{n}\right)\frac{f_2(n\omega')}{f_2(\omega')^n}, \\ P_{11} &= \varepsilon^{1-n}\sqrt{n}\,\frac{\eta(n\omega')}{\eta(\omega')}, \end{aligned}$$

worin ε die in § 33, (15), (18) genau definierte 24ste Einheitswurzel ist.

Nun lassen sich zwei Transformationen

$$\begin{pmatrix}\alpha', \beta'\\ \gamma', \delta'\end{pmatrix}, \quad \begin{pmatrix}a, 0\\ c, \partial\end{pmatrix}, \quad a\partial = n,$$

von denen die erste linear, die andere von der $n$ten Ordnung ist, so bestimmen, daß

$$(7)\qquad \begin{pmatrix}\alpha', & \beta' \\ \gamma', & \delta'\end{pmatrix}\begin{pmatrix}a, & 0 \\ c, & \partial\end{pmatrix} = \begin{pmatrix}1, & 0 \\ 0, & n\end{pmatrix}\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}.$$

Denn schreiben wir die Relation (7) so:

$$\begin{pmatrix}\delta', & -\beta' \\ -\gamma', & \alpha'\end{pmatrix}\begin{pmatrix}1, & 0 \\ 0, & n\end{pmatrix} = \begin{pmatrix}a, & 0 \\ c, & \partial\end{pmatrix}\begin{pmatrix}\delta, & -\beta \\ -\gamma, & \alpha\end{pmatrix},$$

so leitet man daraus einfach her:

$$(8)\qquad \begin{array}{lll}\delta' = a\delta, & \gamma' = \partial\gamma - c\delta, & \\ \partial\beta' = \beta, & n\alpha' = \partial\alpha - c\beta, & a\alpha' = \alpha - c\beta'.\end{array}$$

Hierdurch ist zunächst ∂ bestimmt als der größte gemeinschaftliche Teiler von β und n oder [wegen (4)] von μ' und n. Denn wäre ∂ nicht der größte gemeinschaftliche Teiler von $n = \partial a$ und $\beta = \partial\beta'$, so müßten a und β' einen gemeinsamen Teiler haben und folglich auch β und $\alpha = a\alpha' + c\beta$, was nicht sein kann. Dadurch ist zugleich $a = n/\partial$ bestimmt, und c muß der Kongruenz

$$(9)\qquad \partial\alpha - c\beta \equiv 0 \pmod{n}$$

genügen, wodurch jedoch c nicht absolut, sondern nur nach dem Modul a bestimmt ist. Man kann also c z. B. noch an die Bedingung knüpfen, daß es durch irgend eine Potenz von 2, oder wenn a nicht durch 3 teilbar ist, durch irgend eine Potenz von 3 teilbar sein soll, was wir später bisweilen tun werden.

Die drei Zahlen a, ∂, c können keinen gemeinsamen Teiler haben, denn ein solcher wäre [nach (8)] auch Teiler von α und β, was unmöglich ist. Bezeichnen wir also den größten gemeinsamen Teiler von a und ∂ mit e, so muß c relativ prim zu e sein.

Die Zahlen a, ∂, c, letztere modulo a, sind wegen (4) und (8) durch die beiden Zahlen μ, μ' völlig bestimmt und ändern sich nicht, wenn μ, μ' mit einem gemeinsamen, zu n teilerfremden Faktor multipliziert, d. h. durch ein anderes Paar derselben Reihe ersetzt werden. Zerlegt man n irgendwie in zwei Faktoren a, ∂, so kann man für c noch

$$\frac{a}{e}\,\varphi(e)$$

nach dem Modul a verschiedene zu e teilerfremde Werte annehmen. Jede dieser Annahmen führt zu einem Zahlenpaar μ, μ' durch die Kongruenzen

$$(10) \qquad \begin{aligned} \mu &\equiv \alpha = a\alpha' + c\beta' \\ \mu' &\equiv \beta = \partial\beta' \end{aligned} \pmod{n},$$

worin β' eine beliebige, zu a teilerfremde Zahl bedeutet und α' so bestimmt wird, daß α, β relativ prim werden, und es ist auch leicht [nach § 65, (3)] einzusehen, daß, so lange a, ∂, c dieselben bleiben, die nach (10) bestimmten Zahlenpaare μ, μ' derselben Reihe angehören.

Wir nennen die Zahlen a, c, ∂ (wie in § 27) die Transformationszahlen und n den Transformationsgrad.

Das Zahlensystem a, c, ∂ ist also vollständig charakteristisch für eine Reihe, und die Anzahl der Reihen ist gleich der Anzahl dieser Zahlensysteme, woraus für die Zahl $\psi(n)$, (§ 63) folgt:

$$(11) \qquad \psi(n) = \Sigma \frac{a}{e} \varphi(e),$$

wenn die Summe auf alle Divisoren a von n erstreckt wird.

Es ist von Interesse, diese Relation auch direkt zu beweisen, wobei die Beschränkung auf ein ungerades n wegfallen kann. Betrachten wir $\psi(n)$ jetzt als Zeichen für die Summe (11), so ergibt sich, wenn n', n'' relativ prim sind, zunächst

$$\psi(n')\psi(n'') = \psi(n'n''),$$

und es bleibt also nur übrig, die Summe $\psi(n)$ für den Fall zu bestimmen, daß $n = p^\pi$ eine Primzahlpotenz ist. In diesem Falle ist nun e gleich dem kleineren der beiden Divisoren a, ∂, und wenn $a = \partial$ ist, $e = a$. Wenn wir also das erste und letzte Glied der Summe $\psi(n)$ absondern, so erhalten wir

$$\psi(p^\pi) = 1 + p^\pi + \sum_{1 < a \leqq \sqrt{n}} \varphi(a) + \sum_{\sqrt{n} < a < n} \frac{a}{\partial} \varphi(\partial).$$

Es ist aber

$$\varphi(a) = a\frac{p-1}{p}, \qquad \varphi(\partial) = \partial\frac{p-1}{p},$$

also

$$\psi(p^\pi) = 1 + p^\pi + \frac{p-1}{p} \sum_{1<a<n} a$$

$$= 1 + p^\pi + (p-1)(1 + p + p^2 + \cdots p^{\pi-2}) = p^\pi\left(1 + \frac{1}{p}\right),$$

woraus sich für $\psi(n)$ der Ausdruck

$$\psi(n) = n\,\Pi\left(1+\frac{1}{p}\right)$$

ergibt, wie in § 63 [1]).

Nach (7) ist nun in den Formeln (6) für $n\omega'$ zu setzen:

$$\frac{\gamma' + \delta' \dfrac{c+\partial\omega}{a}}{\alpha' + \beta' \dfrac{c+\partial\omega}{a}},$$

und es lassen sich die linearen Transformationen der f-Funktionen [§ 40, (4), (8), (11)] anwenden. Wir nehmen dabei

(12) $$c \equiv 0 \pmod{16},$$

so daß nach (3) und (8):

$$\begin{pmatrix}\alpha', & \beta' \\ \gamma', & \delta'\end{pmatrix} \equiv \begin{pmatrix}a^3, & 0 \\ 0, & a\end{pmatrix} \pmod{16}.$$

Bezeichnen wir mit ϱ die dritte Einheitswurzel

(13) $$\varrho = e^{-\frac{2\pi i}{3}[\alpha'(\gamma'-\beta')-(\alpha'^2-1)\beta'\delta']}\, e^{\frac{2n\pi i}{3}[\alpha(\gamma-\beta)-(a^2-1)\beta\delta]},$$

so erhalten wir

(14) $$\begin{aligned} P_{00} &= \varrho \quad\;\; \frac{f\left(\dfrac{c+\partial\omega}{a}\right)}{f(\omega)^n}, \\ P_{01} &= \varrho \left(\frac{2}{a}\right) \frac{f_1\left(\dfrac{c+\partial\omega}{a}\right)}{f_1(\omega)^n}, \\ P_{10} &= \varrho \left(\frac{2}{\partial}\right) \frac{f_2\left(\dfrac{c+\partial\omega}{a}\right)}{f_2(\omega)^n}. \end{aligned}$$

Der Quotient

(15) $$\frac{P_{10}}{P_{00}} = \left(\frac{2}{\partial}\right) \frac{f_2\left(\dfrac{c+\partial\omega}{a}\right)}{f\left(\dfrac{c+\partial\omega}{a}\right)} \left(\frac{f\omega}{f_2\omega}\right)^n$$

gibt nach § 54, (3), wenn man

$$u(\omega) = \sqrt[4]{k}$$

setzt, die Größen

---

[1]) Vgl. Dedekind: Über die elliptischen Modulfunktionen. Journal f. Mathematik, Bd. 83.

(16) $$\left(\frac{2}{\partial}\right)\frac{u\left(\dfrac{c+\partial\omega}{a}\right)}{u(\omega)^n}$$

als Wurzeln einer Modulargleichung, und dies ist die Jacobische Modulargleichung [1]).

Ist n nicht durch 3 teilbar, so nehmen wir

(17) $$c \equiv 0 \pmod 3$$

an, wodurch ϱ den Wert 1 erhält.

In gleicher Weise kann man die Transformation der η-Funktion [§ 38, (15), (18), (19)] auf die letzte der Gleichungen (6) anwenden und erhält:

(18) $$P_{11} = \left(\frac{\beta}{\alpha}\right)\left(\frac{\beta'}{\alpha'}\right)\varrho\, i^{\frac{a-1}{2}}\sqrt{\partial}\,\frac{\eta\left(\dfrac{c+\partial\omega}{a}\right)}{\eta(\omega)}$$

(wobei es schon genügen würde, wenn c durch 8 teilbar ist). Ist n durch 3 nicht teilbar und c durch 3 teilbar, so ist auch hierin $\varrho = 1$ zu setzen.

Die Bestimmung des Vorzeichens in (18) hat für uns nur in dem Falle Interesse, wo n ein Quadrat ist. Es ist aber [nach (8)]

$$\left(\frac{\beta}{\alpha}\right)\left(\frac{\beta'}{\alpha'}\right) = \left(\frac{\partial}{\alpha}\right)\left(\frac{\beta'}{\alpha\alpha'}\right) = \left(\frac{\partial}{\alpha}\right)\left(\frac{\beta'}{a}\right) = \left(\frac{\alpha}{\partial}\right)\left(\frac{\beta'}{a}\right)$$

[letzteres nach dem Reziprozitätsgesetz der quadratischen Reste, weil $\alpha \equiv 1 \pmod 4$]. Wenn nun n ein Quadrat ist, so sind auch $a:e$, $\partial:e$ Quadrate und es ergibt sich:

$$\left(\frac{\alpha}{\partial}\right)\left(\frac{\beta'}{a}\right) = \left(\frac{\alpha\beta'}{e}\right) = \left(\frac{c}{e}\right),$$

also wird in diesem Falle

$$P_{11} = \varrho\, i^{\frac{a-1}{2}}\left(\frac{c}{e}\right)\sqrt{\partial}\,\frac{\eta\left(\dfrac{c+\partial\omega}{a}\right)}{\eta(\omega)}.$$

Die zur Charakterisierung einer Reihe aufgestellten Formeln (10) sind ein spezieller Fall eines allgemeineren Systems, das man erhält, indem man auf α', β' in (10) eine lineare Transformation anwendet. Man erhält dann folgendes:

[1]) Ist M der Jacobische Multiplikator, so ist

$$\frac{(kk')^{\frac{n-1}{3}}}{M} = 4^{\frac{n-1}{3}}\, P_{11}^2\, P_{00}^4.$$

Sind a, b, c, ∂ vier der Bedingung:

$$a\partial - bc = n$$

genügende ganze Zahlen ohne gemeinsamen Teiler, so erhält man die einer Reihe entsprechenden Zahlenpaare μ, μ', wenn man in

$$(19) \qquad \begin{matrix} \mu \equiv a\alpha' + c\beta' \\ \mu' \equiv b\alpha' + \partial\beta' \end{matrix} \pmod{n}$$

α', β' alle und nur solche Werte durchlaufen läßt, bei denen μ, μ' ohne gemeinsamen Teiler mit n sind.

Daß zwei den Kongruenzen (19) entsprechende Wertpaare μ, μ' wirklich derselben Reihe angehören, ergibt sich unmittelbar aus § 65 (3), und ebenso ist selbstverständlich, daß alle Zahlenpaare einer Reihe in dieser Form enthalten sind, da man α', β' durch $h\alpha'$, $h\beta'$ ersetzen kann, wenn h relativ prim zu n ist. Daß man sämtliche Reihen auf diesem Wege bekommt, zeigen die Formeln (10).

§ 69. Die Invariantengleichung.

Unter den Transformationsgleichungen verdient eine ein besonderes Interesse, nämlich die, deren Wurzeln die $\psi(n)$ Größen

$$(1) \qquad j\left(\frac{c + \partial\omega}{a}\right)$$

oder nach der Bestimmung (19), § 68 die damit identischen Größen

$$(2) \qquad j\left(\frac{c + \partial\omega}{a + b\omega}\right)$$

sind, wenn $j(\omega)$ die in § 46 definierte Invariante ist.

Diese Gleichung heißt die Invariantengleichung.

Die Funktion $j(\omega)$ läßt sich nach § 54 rational durch $f(\omega)^{24}$ darstellen, nämlich

$$(3) \qquad j(\omega) = \frac{[f(\omega)^{24} - 16]^3}{f(\omega)^{24}},$$

so daß also nach den Resultaten des vorigen Paragraphen die Größen (1) die Wurzeln einer Gleichung sind, deren Koeffizienten rationale Funktionen von $\varkappa^2$ sind.

Setzt man aber für $f(\omega)$ in (3) eine der früher gefundenen Entwickelungen, z. B. § 24, (11):

$$f(\omega) = q^{-\frac{1}{24}} \prod_{1,}^{\nu} (1 + q^{2\nu-1}),$$

so erkennt man, daß $j(\omega)$ sich in eine nach Potenzen von q^2 fortschreitende Reihe entwickeln läßt, welche die Form hat

(4) $$j(\omega) = q^{-2} + a_1 + a_2 q^2 + a_3 q^4 + \cdots,$$

worin die $a_1, a_2, a_3 \ldots$ ganze rationale Zahlen sind, die sich successive berechnen lassen (es ergibt sich z. B. $a_1 = 744$, $a_2 = 196\,884$). Die Entwickelungen der Größen (1) beginnen also mit

(5) $$e^{-\frac{2\pi i c}{a}} e^{-\frac{2\pi i \partial}{a}\omega}$$

und sind daher alle voneinander verschieden. Die Invariantengleichung ist also nach § 65 irreducibel.

Es gibt aber einen zweiten Weg, um zu dieser wie überhaupt zu den Transformationsgleichungen zu gelangen, den wir jetzt zunächst bei der Invariantengleichung kennen lernen wollen. Diese Ableitung stützt sich auf die Sätze des § 54 über Modulfunktionen und gilt auch für ein gerades n. Hier ist es der Satz 4, § 54, der zur Anwendung kommt:

I. Jede Modulfunktion, die durch die beiden Transformationen

(6) $$\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix},$$

(7) $$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

ungeändert bleibt, ist eine rationale Funktion von $j(\omega)$.

Wir weisen zunächst nach, daß durch Anwendung der Substitutionen (6), (7) die ν Größen (1) untereinander vertauscht werden. Wir haben die Zusammensetzung

(8) $$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \lambda, & 1 \end{pmatrix}\begin{pmatrix} a, & 0 \\ c_1, & \partial \end{pmatrix},$$

wenn

(9) $$c_1 = c + \partial - \lambda a$$

gesetzt wird, und es geht durch die Transformation (6), da $j(\omega)$ durch jede lineare Transformation ungeändert bleibt,

$$j\left(\frac{c + \partial\omega}{a}\right) \text{ in } j\left(\frac{c_1 + \partial\omega}{a}\right)$$

über.

Ferner bestimmen wir a_2, ∂_2, c_2, so daß

(10) $$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}\begin{pmatrix} a_2, & 0 \\ c_2, & \partial_2 \end{pmatrix},$$
$$\alpha\delta - \beta\gamma = 1.$$

Dazu ist erforderlich

$$(11)\qquad \begin{aligned} \alpha a_2 + \beta c_2 &= 0 \\ \gamma a_2 + \delta c_2 &= -\partial, \end{aligned}$$

$$(12)\qquad \begin{aligned} \beta \partial_2 &= a \\ \delta \partial_2 &= c. \end{aligned}$$

Es ist also ∂_2 bestimmt als der größte gemeinschaftliche Teiler von a und c, und damit zugleich, wegen $a_2 \partial_2 = n$, auch a_2.

Nach den beiden Gleichungen (12) kennt man jetzt β, δ als relative Primzahlen und kann α, γ aus der diophantischen Gleichung

$$\alpha\delta - \beta\gamma = 1$$

bestimmen. Ist dies geschehen, so folgt aus den beiden Gleichungen (11)

$$(13)\qquad \begin{aligned} a_2 &= \partial \beta, \\ c_2 &= -\partial \alpha, \end{aligned}$$

wodurch auch c_2 bestimmt ist, und es zeigt sich zugleich, daß ∂ der größte gemeinschaftliche Teiler von a_2, c_2 ist. Ersetzt man α, γ durch eine andere Lösung $\alpha + h\beta$, $\gamma + h\delta$, so ändert sich nur c_2 um ein Vielfaches von a_2.

Durch die Transformation (7) geht also

$$j\left(\frac{c + \partial\omega}{a}\right) \text{ in } j\left(\frac{c_2 + \partial_2 \omega}{a_2}\right)$$

über.

Bilden wir nun eine **symmetrische** Funktion der sämtlichen Größen (1), etwa für ein unbestimmtes x das Produkt

$$\Pi\left[x - j\left(\frac{c + \partial\omega}{a}\right)\right],$$

so ändert sich diese Funktion nicht durch die Transformationen (6), (7) und ist also nach dem oben erwähnten Satz eine **rationale Funktion** von $j(\omega)$. Außerdem ist sie eine ganze rationale Funktion νten Grades von x mit dem Anfangsglied x^ν, und wir bezeichnen sie mit $F_n[x, j(\omega)]$. Die Gleichung

$$(14)\qquad F_n[x, j(\omega)] = 0$$

hat die Größen $j\left(\frac{c + \partial\omega}{a}\right)$ zu Wurzeln und ist die **Invariantengleichung**, deren wichtigste Eigenschaften wir nun ableiten wollen.

1. Die Invariantengleichung ist **irreducibel**, wenn als Rationalitätsbereich der Inbegriff aller rationalen Funktionen von

$j(\omega)$ mit beliebigen Zahlenkoeffizienten betrachtet wird. Denn besteht irgend eine rationale Gleichung

$$\Phi[j(n\omega),\ j(\omega)] = 0, \tag{15}$$

so darf darauf jede beliebige lineare Transformation

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$$

angewandt werden, und nach § 29, (5) lassen sich, wenn

$$\begin{pmatrix}a, & b\\ c, & \partial\end{pmatrix}$$

eine beliebige Transformation $n$ter Ordnung ist, die linearen Transformationen

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}, \qquad \begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}$$

immer so bestimmen, daß

$$\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}\begin{pmatrix}a, & b\\ c, & \partial\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & n\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}. \tag{16}$$

Daraus folgt aber, daß die Gleichung (9) durch jede der Größen

$$j\left(\frac{c + \partial\omega}{a + b\omega}\right)$$

und mithin auch durch jede der Größen (1) befriedigt ist, woraus [wegen der Verschiedenheit der Größen (1)] die Irreducibilität von (14) folgt.

2. Die Funktion

$$F_n[x, j(\omega)] = \Pi\left[x - j\left(\frac{c + \partial\omega}{a}\right)\right] \tag{17}$$

hat für jeden endlichen Wert von ω mit positiv imaginärem Bestandteil, also auch für jeden endlichen Wert von $j(\omega)$, einen endlichen Wert und ist sonach eine ganze rationale Funktion von $j(\omega)$.

Suchen wir ferner nach (3) das Anfangsglied der Entwickelung der Funktion (17) nach Potenzen von q, so ergibt sich

$$(-1)^\nu e^{-2\pi i \Sigma \frac{c}{a}} e^{-2\pi i \omega \Sigma \frac{\partial}{e} \varphi(e)} = C q^{-2\nu},$$

wenn C eine endliche Konstante ist. Es ist daher

$$j(\omega)^{-\nu} F_n[x, j(\omega)]$$

für ein unendliches $j(\omega)$ endlich, d. h. der Grad von $F_n[x, j(\omega)]$ in bezug auf $j(\omega)$ ist ebenfalls der νte.

3. Es ist

$$F_n[j(n\omega), j(\omega)] = 0$$

und wenn wir $n\omega$ durch ω ersetzen:

$$F_n\left[j(\omega), j\left(\frac{\omega}{n}\right)\right] = 0.$$

Da nun $j\left(\frac{\omega}{n}\right)$ gleichfalls eine Wurzel der Invariantengleichung ist, so folgt, daß die beiden Gleichungen νten Grades

$$F_n[x, j(\omega)] = 0, \quad F_n[j(\omega), x] = 0$$

eine Wurzel gemeinsam haben, und folglich, wegen der Irreducibilität der ersteren und der Gleichheit des Grades, alle. Es ist daher

$$F_n(x, y) = CF_n(y, x)$$

für unbestimmte Werte der Variablen x, y und ein konstantes C. Daher auch, durch Vertauschung von x mit y:

$$F_n(y, x) = CF_n(x, y),$$

also $C^2 = 1$ oder

$$F_n(x, y) = \pm F_n(y, x).$$

Wenn wir nun $x = y$ setzen, so folgt:

$$F_n(y, y) = \pm F_n(y, y),$$

also, wenn das untere Zeichen gilt,

$$F_n(y, y) = 0.$$

Dies ist aber nur möglich, wenn $n = 1$ ist [wo $F_1(x, y) = x - y$ wird], da sonst $F_n(x, y)$ durch $x - y$ teilbar sein müßte, was der Irreducibilität widerspricht. Daher ist immer, sobald $n > 1$ ist:

(18) $$F_n(x, y) = F_n(y, x).$$

4. Es sei

$$n = n'n'', \quad \nu' = \psi(n'), \quad \nu'' = \psi(n''),$$

und n', n'' ohne gemeinsamen Teiler, und $x_1, x_2, \dots x_{\nu''}$ seien die Wurzeln der Gleichung

(19) $$F_{n''}[x, j(\omega)] = 0.$$

Das Produkt

(20) $$F_{n'}(x, x_1)\, F_{n'}(x, x_2) \dots F_{n'}(x, x_{\nu''}),$$

dessen Grad in bezug auf x gleich

$$\nu = \psi(n) = \psi(n')\,\psi(n'')$$

ist, hängt als symmetrische Funktion der Wurzeln von (19), rational von $j(\omega)$ ab und verschwindet für

$$x = j\left(\frac{\omega}{n'n''}\right),$$

d. h. für eine Wurzel der Gleichung $F_n[x, j(\omega)] = 0$. Wegen der Irreducibilität der letzteren Gleichung, der Gleichheit des Grades und des Koeffizienten von x^ν ist also

$$(21)\qquad F_n[x, j(\omega)] = F_{n'}(x, x_1) F_{n'}(x, x_2) \ldots F_{n'}(x, x_{\nu''}).$$

5. Ist $n = p^\pi$ eine Primzahlpotenz, so ist der Grad der Funktion $F_n[x, j(\omega)]$ gleich $p^{\pi-1}(p+1)$, und die Gleichung

$$(22)\qquad F_{p^{\pi-1}}[x, j(\omega)] = 0$$

ist vom Grade

$$\nu' = p^{\pi-2}(p+1).$$

Wir bezeichnen ihre Wurzeln mit $x_1, x_2, \ldots x_{\nu'}$.

Das Produkt

$$P = F_p(x, x_1) F_p(x, x_2) \ldots F_p(x, x_{\nu'})$$

ist in bezug auf x vom Grade $\nu'(p+1) = p^{\pi-2}(p+1)^2$; es hängt symmetrisch von den Wurzeln von (22), also rational von $j(\omega)$ ab und verschwindet für

$$x = j\left(\frac{\omega}{p^\pi}\right).$$

Daher ist P durch $F_n[x, j(\omega)]$ teilbar.

Aber der Grad von P ist höher als der von F_n. Nehmen wir

$$x_1 = j\left(\frac{p^{\pi-2}c + \omega}{p^{\pi-1}}\right),$$

wo c jeden der Werte $0, 1, 2, \ldots p-1$ haben kann, so verschwindet $F_p(x, x_1)$ für

$$x = j\left(\frac{\omega}{p^{\pi-2}}\right),$$

d. h. es haben p von den Faktoren von P einen bestimmten Faktor mit $F_{p^{\pi-2}}[x, j(\omega)]$ gemein; daraus folgt, daß P durch

$$\{F_{p^{\pi-2}}[x, j(\omega)]\}^p$$

teilbar ist, und mithin, wie die Vergleichung der Grade und höchsten Glieder lehrt:

$$(23)\qquad F_{p^\pi}[x, j(\omega)] = \frac{F_p(x, x_1) F_p(x, x_2) \ldots F_p(x, x_{\nu'})}{\{F_{p^{\pi-2}}[x, j(\omega)]\}^p}.$$

Diese Formel ist einer Ausnahme unterworfen für $\pi = 2$, weil in diesem Falle der Grad der Funktion auf der rechten Seite noch zu hoch ist. Für diesen Fall hat aber jeder der $p+1$ Faktoren des Produktes P den Teiler $x - j(\omega)$, weil eben jedes x_i Wurzel der Gleichung $F_p[x, j(\omega)]$ ist, und es tritt an Stelle von (23) die Formel

$$(24)\qquad F_{p^2}[x, j(\omega)] = \frac{F_p(x, x_1) F_p(x, x_2) \ldots F_p(x, x_{p+1})}{[x - j(\omega)]^{p+1}}.$$

Hierdurch ist die Lösung der Invariantengleichung $F_n = 0$ auf die successive Lösung solcher Fälle zurückgeführt, in denen n eine Primzahl ist.

6. Während bei der Ableitung der Transformationsgleichungen aus den Teilungsgleichungen von Haus aus feststeht, daß die numerischen Koeffizienten in diesen Gleichungen rationale Zahlen sind, so lehrt uns die zweite Ableitung zunächst nichts über die Zahlenkoeffizienten. Wir können aber nachträglich beweisen, daß diese Koeffizienten nicht nur rationale, sondern auch ganze Zahlen sind und gelangen zugleich zu einem wichtigen Satz über die Teilbarkeit dieser Koeffizienten.

Wenn wir beweisen können, daß, wenn p eine Primzahl ist, die Koeffizienten in $F_p(x, y)$ ganze Zahlen sind, so folgt das Gleiche aus 4. und 5. für jedes zusammengesetzte n.

Nach (4) ist $j(\omega)$ in eine Reihe von der Form entwickelbar

$$j(\omega) = q^{-2} \sum_{0,\infty}^{h} a_h q^{2h}, \tag{25}$$

deren Koeffizienten a_h ganze Zahlen sind, und zwar $a_0 = 1$.

Bilden wir hiervon, wenn p eine Primzahl ist, die $p$te Potenz, und beachten den für jede ganze Zahl gültigen Fermatschen Satz:

$$a^p \equiv a \pmod{p},$$

so folgt

$$j(\omega)^p = q^{-2p} \sum_{0,\infty}^{h} a_h q^{2hp} + p\, q^{-2(p-1)} \sum_{0,\infty}^{h} b_h q^{2h}, \tag{26}$$

worin b_h ebenfalls ganze Zahlen sind. Andererseits ist, wenn man in (25) ω durch $p\omega$ ersetzt:

$$j(p\omega) = q^{-2p} \sum_{0,\infty}^{h} a_h q^{2hp} \tag{27}$$

und daraus, wenn man

$$j(\omega) = u, \quad j(p\omega) = v$$

setzt:

$$u^p - v = p\, q^{-2(p-1)} \sum_{0,\infty}^{h} b_h q^{2h},$$

wofür wir auch schreiben können:

$$(u^p - v)(u - v^p) = p\, q^{-2(p^2+p-1)} \sum_{0,\infty}^{h} c_h q^{2h}, \tag{28}$$

wenn c_h ein drittes System ganzer Zahlen bedeutet.

Nun kommen in $F_p(x, y)$ die in bezug auf x, y höchsten Glieder $x^{p+1} + y^{p+1}$ vor, und wir setzen demnach

$$F_p(x, y) = (x^p - y)(x - y^p) - \sum_{0,p}^{h,k} c_{h,k} x^h y^k, \tag{29}$$

worin $c_{h,k}$ die zu bestimmenden Koeffizienten sind, die nach 3. der Bedingung

$$c_{h,k} = c_{k,h}$$

genügen. Um sie zu bestimmen, setzen wir in (29)

$$x = u, \quad y = v,$$

wodurch F_p verschwindet, und erhalten

$$(30) \qquad (u^p - v)(u - v^p) = \sum^{h,k} c_{h,k} u^h v^k.$$

Hieraus folgt zunächst, daß

$$c_{p,p} = 0$$

sein muß, da nach (28) bei der Entwickelung (der linken Seite) nach Potenzen von q die Potenz $q^{-2(p^2+p)}$ nicht vorkommen kann, und wir können (29) jetzt in die Form setzen:

$$(31) \qquad (u^p - v)(u - v^p) = \sum_{0,p}^{h} \sum_{0,h-1}^{k} c_{h,k}(u^h v^k + u^k v^h) + \sum_{0,p-1}^{h} c_{h,h} u^h v^h.$$

Hierin sind die aus (25) und (27) sich ergebenden Entwickelungen von

$$u^h v^k + u^k v^h, \quad u^h v^h$$

nach Potenzen von q einzusetzen, deren Anfangsglieder

$$q^{-2(hp+k)}, \quad q^{-2h(p+1)}$$

die Koeffizienten 1 haben.

Auf der rechten Seite von (31) kommen nicht zwei Glieder vor, deren Entwickelung mit derselben Potenz von q beginnt, denn aus

$$hp + k = h'p + k'$$

folgt $k \equiv k' \pmod{p}$ und mithin, da k und $k' < p$ sind, $k = k'$, $h = h'$.

Ordnet man daher die Reihen, welche die beiden Seiten von (31) darstellen, nach aufsteigenden Potenzen von q, und setzt dann die Koeffizienten gleich hoher Potenzen einander gleich, so erhält man eine Reihe linearer Gleichungen für die Unbekannten $c_{h,k}$, von denen jede folgende nur eine neue Unbekannte enthält, und diese mit dem Koeffizienten 1. Die aus der linken Seite sich ergebenden bekannten Glieder dieser Gleichungen sind nach (28) lauter durch p teilbare ganze Zahlen, und es ergeben sich also für die $c_{h,k}$ ebenfalls ganzzahlige, durch p teilbare Zahlwerte. Demnach haben wir

$$(32) \qquad F_p(x, y) = (x^p - y)(x - y^p) - p \sum_{0,p}^{h,k} a_{h,k} x^h y^k,$$

worin $a_{h,k}$ ganze Zahlen sind, die den Bedingungen

$$a_{h,k} = a_{k,h}, \quad a_{p,p} = 0$$

genügen.

§ 70. Transformationsgleichungen erster Stufe.

Die Invariantengleichung ist von großer theoretischer Wichtigkeit teils wegen ihrer allgemeinen Gültigkeit (auch für gerade n), teils wegen der Leichtigkeit, mit der die linearen Transformationen auf $j(\omega)$ angewandt werden können. Die wirkliche Berechnung dieser Gleichung aber zeigt sich so kompliziert, und die Zahlenkoeffizienten sind so groß, daß die Berechnung bis jetzt nur in dem einfachsten Falle $p = 2$ durchgeführt ist. Dagegen kann man, indem man andere Modulfunktionen benutzt, weit einfachere Transformationsgleichungen erhalten.

Über das hierbei anzuwendende Prinzip bemerken wir folgendes:

Wenn irgend ein System von ν Funktionen von ω vorliegt, entsprechend den ν Systemen von Transformationszahlen a, c, ∂, die wir mit

(1) $$\Phi_{a,c,\partial}$$

bezeichnen wollen und die isomorph mit den Funktionen

(2) $$j\left(\frac{c + \partial\omega}{a}\right)$$

durch die Substitutionen

(3) $$\left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 1)$$

untereinander permutiert werden, so ist (1) rational durch (2) und durch $j(\omega)$ ausdrückbar, denn die Funktion

(4) $$F_n[x, j(\omega)] \sum^{a,c,\partial} \frac{\Phi_{a,c,\partial}}{x - j\left(\frac{c + \partial\omega}{a}\right)} = \Psi[x, j(\omega)]$$

bleibt durch die Substitutionen (3) ungeändert, und ist daher (für ein unbestimmtes x) eine rationale Funktion von $j(\omega)$ und überdies eine ganze rationale Funktion von x, höchstens vom Grade $\nu - 1$; $F_n[x, j(\omega)]$ hat dieselbe Bedeutung, wie in (17) des vorigen Paragraphen, und $\nu = \psi(n)$ ist der Grad dieser Funktion in bezug auf x. Aus (4) aber erhält man, indem man

$$x = j\left(\frac{c + \partial\omega}{a}\right)$$

setzt:

(5) $$\Phi_{a,c,\mathfrak{d}} = \frac{\Psi\left[j\left(\frac{c+\mathfrak{d}\omega}{a}\right), j(\omega)\right]}{F'\left[j\left(\frac{c+\mathfrak{d}\omega}{a}\right)\right]}.$$

Es gehört also $\Phi_{a,c,\mathfrak{d}}$ dem algebraischen Körper an, der aus den rationalen Funktionen von $j\left(\frac{c+\mathfrak{d}\omega}{a}\right)$ und $j(\omega)$ besteht, und wir können die Sätze von Bd. I, § 151 anwenden. Aus diesen folgt, daß die ν Größen $\Phi_{a,c,\mathfrak{d}}$ die Wurzeln einer Gleichung νten Grades sind, deren Koeffizienten rational von $j(\omega)$ abhängen. Wenn die ν Größen $\Phi_{a,c,\mathfrak{d}}$ voneinander verschieden sind, so ist diese Gleichung irreducibel. Eine solche Gleichung nennen wir eine zum Transformationsgrad n gehörige Transformationsgleichung erster Stufe[1]). Jede andere Größe des Körpers kann durch ein solches $\Phi_{a,c,\mathfrak{d}}$ und durch $j(\omega)$ rational ausgedrückt werden.

Haben die Funktionen $\Phi_{a,c,\mathfrak{d}}$ die Eigenschaft, für jeden endlichen Wert von ω mit positivem, imaginärem Teil, also für jedes endliche $j(\omega)$ endlich zu bleiben, so ist die Funktion $\Psi[x, j(\omega)]$ in (4) auch in bezug auf $j(\omega)$ eine ganze Funktion. Die Formel (5) könnte daher nur für solche besondere Werte von ω versagen, für die zwei Wurzeln der Invariantengleichung einander gleich werden.

Wenn die ν Größen $\Phi_{a,c,\mathfrak{d}}$ nicht alle voneinander verschieden sind, so zerfallen sie in Reihen von gleich vielen untereinander gleichen, und die aus (5) abzuleitende Gleichung νten Grades ist eine Potenz einer irreducibeln Gleichung, die wir gelegentlich wohl auch als Transformationsgleichung bezeichnen werden (Bd. I, § 151, 2).

Sind die Größen $\Phi_{a,c,\mathfrak{d}}$ so gewählt, daß sie für kein endliches ω mit positiv imaginärem Bestandteil unendlich werden, so bleiben sie für jedes endliche $j(\omega)$ endlich, woraus folgt, daß die Koeffizienten in der Funktion des νten Grades

(6) $$\Pi(x - \Phi_{a,c,\mathfrak{d}})$$

ganze rationale Funktionen von $j(\omega)$ sind, d. h. die $\Phi_{a,c,\mathfrak{d}}$ sind ganze algebraische Funktionen von $j(\omega)$.

---

[1]) In der ersten Auflage habe ich diese Gleichungen „invariante Transformationsgleichungen" genannt. Dieser Ausdruck ist von Klein beanstandet worden (Vorlesungen über ausgewählte Kapitel der Zahlentheorie, autographiertes Heft, Göttingen 1897). Ich schließe mich Kleins Vorschlag an, indem ich diese Gleichungen jetzt „Transformationsgleichungen erster Stufe" nenne, ohne hier näher auf die Begründung dieses Ausdruckes einzugehen.

Richtet man die Funktionen $\Phi_{a, c, \partial}$, etwa durch geeignete Bestimmung von Konstanten, die darin noch verfügbar sind, so ein, daß sie auch für ein unendliches imaginäres ω, d. h. für $q = 0$ endlich bleiben, so sind diese Funktionen auch für ein unendliches $j(\omega)$ endlich, und die Koeffizienten in (6) sind konstant. Dies ist aber nur dadurch möglich, daß die $\Phi_{a, c, \partial}$ alle einer und derselben Konstanten C gleich sind. Kennt man $\Phi_{a, c, \partial}$ als rationale Funktion einer anderen Größe $\Psi_{a, c, \partial}$, so ist $\Phi_{a, c, \partial} = C$ entweder eine Identität oder eine Transformationsgleichung für $\Psi_{a, c, \partial}$.

§ 71. Die Transformationsgleichungen für γ_2 und γ_3.

Transformationsgleichungen erster Stufe erhält man zunächst aus der Betrachtung der Funktionen § 54, (4), (5):

$$\gamma_2(\omega) = \sqrt[3]{j(\omega)}, \quad \gamma_3(\omega) = \sqrt{j(\omega) - 1728}.$$

Wenn n nicht durch 3 teilbar ist, so können wir die Zahlen a, c, ∂ so wählen, daß immer c durch 3 teilbar wird.

Nun übt nach § 54, (15) eine lineare Transformation $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ auf die Funktion $\gamma_2(\omega)$ den Einfluß:

$$\gamma_2\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = e^{-\frac{2\pi i}{3}(\alpha\gamma + \beta\delta - \alpha\beta - \alpha^2\beta\delta)}\,\gamma_2(\omega).$$

In den Zusammensetzungen (8), (10) des § 69 wird

$$\lambda \equiv n, \quad \delta \equiv 0 \pmod 3,$$

und dann kann man α noch so bestimmen, daß auch α und folglich c_2 durch 3 teilbar werden.

Daraus ergibt sich, daß durch die beiden Substitutionen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

die ν Funktionen

$$\gamma_2\left(\frac{c + \partial\omega}{a}\right)\gamma_2(\omega)^{-n} \tag{1}$$

nur untereinander vertauscht werden und also die Wurzeln einer Transformationsgleichung erster Stufe sind.

Ist zweitens n eine ungerade Zahl, so nehme man c gerade an.

Für die Funktion $\gamma_3(\omega)$ ist [nach § 54, (15)]:

$$\gamma_3\left(\frac{\gamma + \delta\omega}{\alpha + \beta\omega}\right) = (-1)^{\alpha\gamma + \beta\gamma + \beta\delta}\gamma_3(\omega),$$

und in den Zusammensetzungen (8), (10), § 69 ist

$$\lambda \equiv 1, \quad \alpha \equiv \delta \equiv 0 \pmod{2}.$$

Die ν Größen

(2) $$\gamma_3\left(\frac{c + \partial\omega}{a}\right)\gamma_3(\omega)$$

vertauschen sich daher untereinander und sind also gleichfalls die Wurzeln einer Transformationsgleichung erster Stufe.

Um für den einfachsten Fall $n = 2$ die erstere dieser Gleichungen zu bilden, beachte man die Relation [§ 54, (5)]:

(3) $$\gamma_2(\omega) = \frac{f(\omega)^{24} - 16}{f(\omega)^8} = \frac{f_1(\omega)^{24} + 16}{f_1(\omega)^8} = \frac{f_2(\omega)^{24} + 16}{f_2(\omega)^8},$$

woraus wegen

$$f_1(2\omega)f_2(\omega) = \sqrt{2} \qquad \text{[§ 34, (16)]}$$

folgt:

(4) $$\begin{aligned} \gamma_2(2\omega) &= \frac{2^8 + f_2(\omega)^{24}}{f_2(\omega)^{16}} \\ \gamma_2\left(\frac{\omega}{2}\right) &= \frac{2^8 + f_1(\omega)^{24}}{f_1(\omega)^{16}} \\ \gamma_2\left(\frac{\omega + 3}{2}\right) &= \frac{2^8 - f(\omega)^{24}}{f(\omega)^{16}}. \end{aligned} \qquad \text{[§ 34, (13)]}$$

Bezeichnen wir diese drei Größen mit x, x_0, x_1, so ergibt sich aus den Relationen (6), (8), § 54:

$$\begin{aligned} x + x_0 + x_1 &= \gamma_2(\omega)^2 \\ xx_0 + xx_1 + x_0x_1 &= 495\,\gamma_2(\omega) \\ xx_0x_1 &= -j(\omega) + 2^4.3^3.5^3, \end{aligned}$$

so daß x, x_0, x_1 die Wurzeln der Gleichung sind

(5) $$x^3 - \gamma_2(\omega)^2x^2 + 5.9.11.\gamma_2(\omega)x + j(\omega) - 2^4.3^3.5^3 = 0.$$

Die Gleichung, deren Wurzeln die Kuben der Wurzeln von (5) sind, ist die Invariantengleichung für $n = 2$, und läßt sich daraus ohne Schwierigkeit berechnen.

§ 72. Multiplikatorgleichungen erster Stufe.

Unter den Multiplikatorgleichungen sollen hier die betrachtet werden, deren Wurzeln die verschiedenen Potenzen von P_{11} sind, multipliziert mit Potenzen von $\gamma_2(\omega)$, $\gamma_3(\omega)$, deren Koeffizienten

rational von $j(\omega)$ abhängen. Diese Gleichungen nennen wir **Multiplikatorgleichungen erster Stufe**[1]).

Wir betrachten die Größen [§ 68, (16)]:

$$(1)\qquad P_{c,\delta,a} = i^{\frac{a-1}{2}} \left(\frac{c}{e}\right) \sqrt{\delta}\, \frac{\eta\left(\frac{c+\delta\,\omega}{a}\right)}{\eta(\omega)},$$

und den Einfluß, den die Transformationen

$$\begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \quad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

auf sie ausüben. Dieser Einfluß bestimmt sich nach den Formeln (8) bis (13), § 69, wonach [weil $c_1 \equiv c \pmod{e}$]

$$P_{c,\delta,a} \text{ durch } (\omega, \omega + 1) \text{ in } e^{\frac{\pi i(\lambda-1)}{12}} P_{c_1,\delta,a}$$

$$(2)\qquad \text{durch } \left(\omega, -\frac{1}{\omega}\right)$$

$$\text{in } \sqrt{\frac{\delta}{\delta_2}}\, \frac{i^{\frac{a-a_2}{2}}}{\sqrt{-i\omega}} \left(\frac{c}{e}\right) \left(\frac{c_2}{e_2}\right) E\begin{pmatrix} \alpha, & \beta & \frac{c_2 + \delta_2\,\omega}{a_2} \\ \gamma, & \delta' & \end{pmatrix} P_{c_2,\delta_2,a_2}$$

übergeht, worin E die in § 38, (15) angegebene Bedeutung hat. Es ist aber [§ 69, (11), (12)]

$$\sqrt{\delta} \sqrt{\alpha + \beta\, \frac{c_2 + \delta_2\,\omega}{a_2}} = \sqrt{\delta_2\,\omega},$$

und mithin, wenn wir

$$E\begin{pmatrix} \alpha, & \beta & \frac{c_2 + \delta_2\,\omega}{a_2} \\ \gamma, & \delta' & \end{pmatrix} = r\sqrt{-i\omega}\sqrt{\frac{\delta_2}{\delta}}$$

setzen,

$$r = \left(\frac{\alpha}{\beta}\right) i^{\frac{1-\beta}{2}} e^{\frac{\pi i}{12}[\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma]}$$

eine **24ste Einheitswurzel**, und durch die Vertauschung

$$\left(\omega, -\frac{1}{\omega}\right)$$

geht

$$P_{c,\delta,a} \text{ in } r\, i^{\frac{a-a_2}{2}} \left(\frac{c}{e}\right) \left(\frac{c_2}{e_2}\right) P_{c_2,\delta_2,a_2}$$

über.

---

[1]) Diese Gleichungen sind besonders eingehend von Kiepert untersucht worden, zuerst in mehreren Abhandlungen in Crelles Journal, Bd. 87, 88, 95, am ausführlichsten in den Abhandlungen in den Mathematischen Annalen, Bd. 26, 33. Vgl. auch F. Klein, Mathematische Annalen, Bd. 14, 15 und die oben erwähnten autographierten Vorlesungen.

Daraus ergibt sich wie oben der Schluß:

1. Für jedes beliebige n sind die Größen

$$P^{24}_{c, \mathfrak{d}, a}$$

die Wurzeln einer Transformationsgleichung.

Ist n durch 3 nicht teilbar, so kann man die c, c_2, c_1 durch 3 teilbar voraussetzen. Dann wird

$$\lambda \equiv n, \quad \alpha \equiv 0, \quad \delta \equiv 0 \pmod 3.$$

Es ist also, wie aus § 38, (15) hervorgeht, r eine achte Einheitswurzel, beachtet man daher noch

$$\gamma_2(\omega + 1) = e^{-\frac{2\pi i}{3}} \gamma_2(\omega), \quad \gamma_2\left(-\frac{1}{\omega}\right) = \gamma_2(\omega), \quad [\text{§ 54, (14)}]$$

so haben wir den Satz:

2. Ist n nicht durch 3 teilbar und c durch 3 teilbar, so sind die Größen

$$P^{8}_{c, \mathfrak{d}, a}\, \gamma_2(\omega)^{n-1}$$

Wurzeln einer Transformationsgleichung.

Um die Anwendung auf den einfachsten Fall $n = 2$ zu machen, setzen wir

$$(3) \qquad x = 16\,\frac{\eta(2\omega)^8}{\eta(\omega)^8}, \quad x_0 = \frac{\eta\left(\frac{\omega}{2}\right)^8}{\eta(\omega)^8}, \quad x_1 = \frac{\eta\left(\frac{\omega+3}{2}\right)^8}{\eta(\omega)^8},$$

und dann sind x, x_0, x_1 nichts anderes als unsere Funktionen

$$f_2(\omega)^8, \quad f_1(\omega)^8, \quad -f(\omega)^8. \qquad [\text{§ 34, (9)}]$$

Diese sind, wie wir schon früher gesehen haben [§ 54, (8)], die Wurzeln der kubischen Gleichung

$$(4) \qquad x^3 - x\gamma_2(\omega) + 16 = 0.$$

Der Umstand, daß f_2^8, f_1^8, $-f^8$ selbst Wurzeln einer Transformationsgleichung für den Transformationsgrad 2 sind, erklärt die Erscheinung, daß bei Adjunktion dieser Größen, also auch bei Adjunktion von $\varkappa^2$, die zu einem geraden n gehörigen Transformationsgleichungen reducibel werden.

Wenn n eine ungerade Zahl ist, so nehme man c durch 4 teilbar an, dann ist [§ 69, (9), (11), (12)]

$$\lambda \equiv n \pmod 4,$$

$$\alpha \equiv 0, \quad \delta \equiv 0, \quad \beta \equiv a\mathfrak{d}_2, \quad \gamma \equiv -\mathfrak{d}\, a_2 \pmod 4,$$

also ergibt sich

$$r^6 = (-1)^{\frac{\beta-1}{2}} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{a-a_2}{2}}$$

und daraus folgt mit Rücksicht auf

$$\gamma_3(\omega+1) = -\gamma_3(\omega), \quad \gamma_3\left(-\frac{1}{\omega}\right) = -\gamma_3(\omega): \qquad [\S\ 54,\ (14)]$$

3. Ist n ungerade, c durch 4 teilbar, so sind die Größen

$$P^6_{c,\mathfrak{d},a}\,\gamma_3(\omega)^{\frac{n-1}{2}}$$

Wurzeln einer Multiplikatorgleichung. Ist $n \equiv 1 \pmod 4$, so gilt dasselbe von $P^6_{c,\mathfrak{d},a}$.

Als Beispiel wählen wir $n = 3$ und setzen

$$(5)\qquad \begin{aligned} x &= 27\left(\frac{\eta(3\omega)}{\eta(\omega)}\right)^6, & x_0 &= -\left(\frac{\eta\left(\frac{\omega}{3}\right)}{\eta(\omega)}\right)^6, \\ x_1 &= -\left(\frac{\eta\left(\frac{4+\omega}{3}\right)}{\eta(\omega)}\right)^6, & x_2 &= -\left(\frac{\eta\left(\frac{8+\omega}{3}\right)}{\eta(\omega)}\right)^6. \end{aligned}$$

Die Koeffizienten der Gleichung, die diese Größen zu Wurzeln hat, sind rationale Funktionen von $\gamma_3(\omega)$, und da keine der Größen (5) für einen endlichen Wert von γ_3 unendlich wird, so sind es ganze Funktionen von γ_3. Nach 3. können wir diese Gleichung also in der Form ansetzen:

$$x^4 + A_1\gamma_3 x^3 + A_2 x^2 + A_3\gamma_3 x + A_4 = 0,$$

worin A_1, A_2, A_3, A_4 ganze rationale Funktionen von $j(\omega)$ sind. Zunächst erhält man A_4 als das Produkt $x x_0 x_1 x_2$, welches für keinen Wert von $j(\omega)$ verschwinden kann und daher konstant sein muß. Aus den Anfängen der Entwickelung [§ 24]

$$(6)\qquad \begin{aligned} x &= 27\,q\ldots, \\ x_0 &= -q^{-\frac{1}{3}}\ldots, \\ x_1 &= -e^{\frac{2\pi i}{3}}\,q^{-\frac{1}{3}}\ldots, \\ x_2 &= -e^{-\frac{2\pi i}{3}}\,q^{-\frac{1}{3}}\ldots, \\ \gamma_3 &= q^{-1}\ldots \end{aligned}$$

findet man daher

$$A_4 = -27.$$

Es ist ferner

$$-A_1\gamma_3 = x + x_0 + x_1 + x_2.$$

Da die rechte Seite für ein unendliches γ_3, d. h. für $q = 0$, nicht einmal in der ersten Ordnung unendlich wird, so muß A_1 verschwinden.

Aus

$$-A_3\gamma_3 = x x_0 x_1 x_2 \left(\frac{1}{x} + \frac{1}{x_0} + \frac{1}{x_1} + \frac{1}{x_2}\right)$$

ergibt sich nach (6) für A_3 der konstante Wert 1. Um aber A_2 zu bestimmen, müssen wir in der Entwickelung noch um ein Glied weiter gehen. Wir setzen in

$$x_0^4 + \gamma_3 x_0 - 27 = -A_2 x_0^2$$

für x_0 die Entwickelung

$$x_0 = -q^{-\frac{1}{3}} + 6 q^{\frac{1}{3}} + \cdots,$$

und finden $A_2 = 18$, so daß also die gesuchte Gleichung lautet:

(7) $$x^4 + 18 x^2 + \gamma_3 x - 27 = 0.$$

Ist n ungerade und nicht durch 3 teilbar, so nehme man c durch 12 teilbar an.

Es ist alsdann

$$\lambda \equiv n, \quad \alpha \equiv 0, \quad \delta \equiv 0, \quad \beta \equiv a\partial_2, \quad \gamma \equiv -\partial a_2 \pmod{12}$$

und es wird

$$r^2 = (-1)^{\frac{\beta-1}{2}} = (-1)^{\frac{n-1}{2}} (-1)^{\frac{a-a'}{2}},$$

also der Satz

4. Ist n relativ prim zu 6, c durch 12 teilbar, so sind die Größen

$$P^2_{c,\partial,a}\gamma_2(\omega)^{n-1}\gamma_3(\omega)^{\frac{n-1}{2}}$$

Wurzeln einer Multiplikatorgleichung erster Stufe.

Da die Funktionen P^2 für keinen endlichen Wert von $j(\omega)$ unendlich oder Null werden, so schließen wir, daß die Koeffizienten der Gleichung, deren Wurzeln die P^2 sind, ganze rationale Funktionen von γ_2, γ_3 sind und daß der letzte Koeffizient eine Konstante ist.

Ist n eine Primzahl p, so sind die Wurzeln dieser Gleichung

$$x = p\left(\frac{\eta(p\omega)}{\eta(\omega)}\right)^2, \quad x_h = (-1)^{\frac{p-1}{2}} \left(\frac{\eta\left(\frac{12h+\omega}{p}\right)}{\eta(\omega)}\right)^2 \quad h = 0, 1, \ldots, p-1$$

und die Anfangsglieder der Entwickelungen sind folgende:

$$x = p q^{\frac{p-1}{6}} \ldots, \quad x_h = (-1)^{\frac{p-1}{2}} e^{\frac{2\pi i h}{p}} q^{-\frac{p-1}{6p}} \ldots,$$

wodurch sich für den letzten Koeffizienten der Wert $(-1)^{\frac{p-1}{2}} p$ ergibt. Daraus, daß das erste Glied in der Entwickelung von

$j(\omega)$ nach Potenzen von q den Koeffizienten 1 hat, schließt man leicht, daß die numerischen Koeffizienten in diesen Gleichungen rationale ganze Zahlen sind.

Für $p = 5$ hat die fragliche Gleichung die Form:

$$x^6 + A_1 \gamma_2^2 x^5 + A_2 \gamma_2 x^4 + A_3 x^3 + A_4 \gamma_2 x + 5 = 0,$$

worin die A_1, A_2, A_3, A_4 ganze rationale Funktionen von $j(\omega)$ und, wie leicht zu sehen, Konstante sind.

Aus den Anfangsgliedern ergibt sich sofort

$$A_1 = 0, \quad A_2 = 0, \quad A_4 = -1.$$

Um aber A_3 zu bestimmen, geht man in der Entwickelung von x_0 bis zum nächstfolgenden Gliede:

$$x_0 = q^{-\frac{7}{15}}\left(1 - 2q^{\frac{2}{5}} \ldots\right),$$

woraus man $A_3 = 10$ erhält; also lautet für $n = 5$ die Multiplikatorgleichung

$$x^6 + 10x^3 - \gamma_2 x + 5 = 0. \tag{8}$$

In gleicher Weise berechnet man die Gleichungen für $p = 7$, $p = 11$, indem man die Entwickelungen von x_0 benutzt:

$$p = 7{:}\ \ x_0 = -q^{-\frac{1}{7}}\left(1 - 2q^{\frac{2}{7}} - q^{\frac{4}{7}} + 2q^{\frac{6}{7}} \ldots\right),$$

$$p = 11{:}\ \ x_0 = -q^{-\frac{5}{33}}\left(1 - 2q^{\frac{2}{11}} - q^{\frac{4}{11}} + 2q^{\frac{6}{11}} + q^{\frac{8}{11}} + 2q^{\frac{10}{11}} + \cdots\right),$$

während von $\gamma_2(\omega)$, $\gamma_3(\omega)$ immer nur die ersten Glieder gebraucht werden. So findet sich

$$p = 7{:}\ \ x^8 + 7.2x^6 + 7.9x^4 + 7.10x^2 + \gamma_3 x - 7 = 0, \tag{9}$$

$$p = 11{:}\ \ x^{12} - 11.90x^6 + 11.40\gamma_2 x^4 + 11.15\gamma_3 x^3 + 11.2\gamma_2^2 x^2 + \gamma_2\gamma_3 x - 11 = 0. \tag{10}$$

Wenn n eine ungerade Quadratzahl ist, so nehmen wir c durch 8 teilbar an. Es sind dann $a:e$ und $\partial:e$ ebenfalls Quadratzahlen. Es ist ferner

$$\alpha \equiv \delta \equiv 0 \pmod 8, \quad \lambda \equiv 1 \pmod 8 \tag{11}$$

$$\left.\begin{array}{lll} a = \beta\partial_2, & a_2 = \beta\partial, & a \equiv \partial \equiv e \equiv 1 \\ c = \delta\partial_2, & c_2 = -\alpha\partial, & a_2 \equiv \partial_2 \equiv e_2 \equiv 1 \end{array}\right\} \pmod 8. \tag{12}$$

Die Einheitswurzel r in (2) erhält den Wert

$$r = \left(\frac{\alpha}{\beta}\right) i^{\frac{1-\beta}{2}} e^{\frac{2\pi i}{3\Delta}\frac{\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma}{8}}. \tag{13}$$

Es ist aber nach (12) β sowohl durch e als auch durch e_2 teilbar und $\beta e e_2$ ein Quadrat; also

$$\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{e e_2}\right) = \left(\frac{\alpha}{e}\right)\left(\frac{\alpha}{e_2}\right) = \left(\frac{\delta}{e}\right)\left(\frac{\alpha}{e_2}\right) \text{ (wegen } \alpha\delta \equiv 1 \bmod e);$$

ferner ist nach (12)

$$\left(\frac{\delta}{e}\right) = \left(\frac{c}{e}\right)\left(\frac{\mathfrak{d}_2}{e}\right), \qquad \left(\frac{\alpha}{e_2}\right) = \left(\frac{c_2}{e_2}\right)\left(\frac{-\mathfrak{d}}{e_2}\right),$$

und

$$\left(\frac{\mathfrak{d}_2}{e}\right) = \left(\frac{e_2}{e}\right), \quad \left(\frac{-\mathfrak{d}}{e_2}\right) = \left(\frac{-e}{e_2}\right), \quad \left(\frac{e_2}{e}\right)\left(\frac{-e}{e_2}\right) = (-1)^{\frac{(e+1)(e_2-1)}{4}},$$

also

$$\left(\frac{\alpha}{\beta}\right) = (-1)^{\frac{(e+1)(e_2-1)}{4}} \left(\frac{c}{e}\right)\left(\frac{c_2}{e_2}\right)$$

$$i^{\frac{1-\beta}{2}} = i^{\frac{1-ee_2}{2}}; \quad i^{\frac{a-a_2}{2}} = i^{\frac{e-e_2}{2}}.$$

Durch die Vertauschungen (2) geht also

$$(14) \quad P_{c,\mathfrak{d},a} \text{ in } e^{\frac{2\pi i}{3}\frac{\lambda-1}{8}} P_{c_1,\mathfrak{d},a} \text{ und in } e^{\frac{2\pi i}{8}\frac{\beta(\alpha+\delta)-(\beta^2-1)\alpha\gamma}{8}} P_{c_2,\mathfrak{d}_2,a_2}$$

über.

Ist n noch durch 3 unteilbar, so nehme man c durch 3 teilbar an, wodurch

$$\lambda \equiv 1, \quad \alpha \equiv \delta \equiv 0 \pmod 3)$$

werden und die in (14) vorkommenden dritten Einheitswurzeln den Wert 1 erhalten.

Hieraus ergeben sich die Sätze:

5. Ist n eine ungerade Quadratzahl, c durch 8 teilbar, so sind die Größen

$$P^3_{c,\mathfrak{d},a},$$

und ist n eine durch 3 nicht teilbare ungerade Quadratzahl, c durch 24 teilbar, so sind die Größen

$$P_{c,\mathfrak{d},a}$$

Wurzeln von Multiplikatorgleichungen erster Stufe.

Die ersten Beispiele sind $n = 9$, $n = 25$.

Zur Bildung dieser Gleichungen kann man auf verschiedene Arten gelangen. Wir wollen hier [nach Kiepert[1])] den Weg gehen, daß wir nach § 69 die Wurzeln einer zum Grade p ge-

[1]) Zur Transformationstheorie der elliptischen Funktionen. Crelles Journal, Bd. 87, 88, 95.

hörenden Transformationsgleichung durch die für den Grad p^2 rational ausdrücken und diesen Ausdruck in die zu p gehörige Transformationsgleichung einsetzen.

Nach 3., Formel (7) wird die Gleichung

$$x^4 + 18x^2 + \gamma_3(\omega)x - 27 = 0 \tag{15}$$

von den beiden Funktionen

$$-\left(\frac{\eta\left(\frac{\omega}{3}\right)}{\eta(\omega)}\right)^6, \quad 27\left(\frac{\eta(3\omega)}{\eta(\omega)}\right)^6 \tag{16}$$

befriedigt. Bezeichnen wir den ersten dieser Werte mit x, so geht der zweite durch die Substitution $\left(\omega, \frac{\omega}{3}\right)$ in $\frac{-27}{x}$ über, und folglich wird durch x auch die Gleichung

$$27^3 + 18.27x^2 - \gamma_3\left(\frac{\omega}{3}\right)x^3 - x^4 = 0 \tag{17}$$

befriedigt. Setzen wir nun

$$y = \left(\frac{\eta\left(\frac{\omega}{9}\right)}{\eta(\omega)}\right)^3, \tag{18}$$

so geht x durch die Substitution $\left(\omega, \frac{\omega}{3}\right)$ in $\frac{y^2}{x}$ über, so daß man auch die Gleichung erhält:

$$y^8 + 18y^4x^2 + \gamma_3\left(\frac{\omega}{3}\right)y^2x^3 - 27x^4 = 0, \tag{19}$$

und durch Elimination von $\gamma_3\left(\frac{\omega}{3}\right)$ aus (17) und (19) erhält man nach Weghebung des Faktors $y^2 + 27$

$$x^4 - 18x^2y^2 - y^2(y^4 - 27y^2 + 27^2) = 0. \tag{20}$$

Löst man diese quadratische Gleichung nach x^2 auf, so folgt:

$$x^2 = y^3 + 9y^2 + 27y = (y+3)^3 - 27, \tag{21}$$

wo über das Zeichen durch Einsetzen der Anfangsglieder der Entwickelungen entschieden wird, am einfachsten wohl, da diese Gleichung (nach § 69) auch für

$$x = 27\left(\frac{\eta(3\omega)}{\eta(\omega)}\right)^6, \quad y = 27\left(\frac{\eta(9\omega)}{\eta(\omega)}\right)^3$$

erfüllt wird, indem man

$$x = 27q + \cdots, \quad y = 27q^2 + \cdots$$

setzt.

Sondert man in (15) die erste Potenz von x ab und erhebt ins Quadrat, so erhält man durch Einsetzen von (21) die gesuchte Multiplikatorgleichung für den 9ten Transformationsgrad. Sie erhält eine einfachere Gestalt, wenn man

$$(y + 3)^3 = t \tag{22}$$

setzt:

$$[j(\omega) - 27.64](t - 27) = (t^2 - 36t + 27.8)^2 \tag{23}$$

oder

$$j(\omega)(t - 27) = t(t - 24)^3. \tag{24}$$

Ganz ähnlich kann man beim 25sten Transformationsgrad verfahren.

Wenn wir

$$x = \left(\frac{\eta\left(\frac{\omega}{5}\right)}{\eta(\omega)}\right)^2, \quad y = \frac{\eta\left(\frac{\omega}{25}\right)}{\eta(\omega)} \tag{25}$$

setzen, so haben wir zunächst nach 4. (8):

$$x^6 + 10x^3 - \gamma_2(\omega)x + 5 = 0, \tag{26}$$

woraus, wie oben, die beiden Gleichungen

$$5^5 + 10.5^2x^3 - \gamma_2\left(\frac{\omega}{5}\right)x^5 + x^6 = 0,$$

$$y^{12} + 10y^6x^3 - \gamma_2\left(\frac{\omega}{5}\right)y^2x^5 + 5x^6 = 0,$$

und durch Elimination von $\gamma_2\left(\frac{\omega}{5}\right)$

$$x^6 - 10x^3y^2(5 + y^2) = y^2(y^8 + 5y^6 + 5^2y^4 + 5^3y^2 + 5^4).$$

Diese Gleichung nach x^3 aufgelöst, ergibt:

$$x^3 = y^5 + 5y^4 + 15y^3 + 25y^2 + 25y, \tag{27}$$

und wenn wir zur Abkürzung die rechte Seite dieser Gleichung mit $\chi(y)$ bezeichnen, nach (26)

$$j(\omega)\chi(y) = [\chi(y)^2 + 10\chi(y) + 5]^3. \tag{28}$$

Dies ist die gesuchte Gleichung 30sten Grades für y.

§ 73. Die Schlaeflischen Modulargleichungen.

Zu einfacheren Transformationsgleichungen gelangt man, wenn man dem Rationalitätsbereich, der bis jetzt aus den rationalen Funktionen von $j(\omega)$ bestand, die Größe $f(\omega)^{24}$ adjungiert. Diesem

Rationalitätsbereich gehören die Funktionen von ω an, die durch die beiden Substitutionen

$$(1) \qquad \left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 2)$$

ungeändert bleiben (§ 54, 2). Wenn also ein System von ν Funktionen $\Phi_{a,c,\partial}$ durch die Substitutionen (1) nur unter sich permutiert wird, so sind diese Funktionen die Wurzeln einer Transformationsgleichung, deren Koeffizienten rational von $f(\omega)^{24}$ abhängen. Hierzu gehören (wie wir früher schon auf anderem Wege nachgewiesen haben) für ein ungerades n, das wir jetzt immer voraussetzen, gewisse Potenzen der Größen

$$f\left(\frac{c + \partial\omega}{a}\right),$$

worin, wie ein- für allemal bemerkt sei, c durch 16, und wenn n nicht durch 3 teilbar ist, durch 48 teilbar angenommen wird.

Die etwas erweiterten Grundsätze des § 70 führen verhältnismäßig einfach zur Berechnung dieser Gleichungen.

Eine Erweiterung ist aber notwendig aus folgendem Grunde:

Bei den bisherigen Betrachtungen konnten wir den Schluß machen: wenn eine rationale Funktion von $j(\omega)$ für jedes endliche ω mit positiv imaginärem Teil endlich bleibt, so ist sie eine ganze Funktion von $j(\omega)$, weil zu jedem endlichen $j(\omega)$ auch ein endliches, nicht reelles ω gehört (§ 52). Bei den rationalen Funktionen von $f(\omega)$ können wir aber aus der Endlichkeit für jedes endliche imaginäre ω nur schließen, daß sie ganze Funktionen von $f(\omega)$ und $1:f(\omega)$ sind, weil nur zu jedem endlichen $f(\omega)$ mit Ausnahme von $f(\omega) = 0$ ein endliches imaginäres ω gehört.

Es entspricht aber der Substitution

$$(2) \qquad \left(\omega, \frac{\omega - 1}{\omega + 1}\right)$$

die Vertauschung

$$\left(f(\omega), \frac{\sqrt{2}}{f(\omega)}\right), \qquad [§ 34, (18)]$$

und wenn also die Funktionen $\Phi_{a,c,\partial}$ so gewählt sind, daß sie auch durch die Substitution (2) nur untereinander permutiert werden, so werden die Koeffizienten der Gleichung, deren Wurzeln sie sind, rational von

$$f(\omega) + \frac{\sqrt{2}}{f(\omega)}$$

abhängen. Sie sind ganze Funktionen dieser Verbindungen, wenn die $\Phi_{a,c,\partial}$ für jedes endliche, nicht reelle ω endlich bleiben, und sie sind konstant, wenn alle $\Phi_{a,c,\partial}$ auch für $q = 0$, d. h. für $f(\omega) = 0$ und $f(\omega) = \infty$, endlich bleiben. In diesem Falle sind sämtliche $\Phi_{a,c,\partial}$ einer und derselben Konstanten gleich (§ 70).

Daraus ergibt sich der Satz:

Bildet man ganze rationale Funktionen $\Phi_{a,c,\partial}$ aus

$$f\left(\frac{c + \partial\omega}{a}\right), \quad f(\omega), \quad \frac{1}{f\left(\frac{c + \partial\omega}{a}\right)}, \quad \frac{1}{f(\omega)},$$

welche die Eigenschaft haben:

1. durch die Substitutionen

$$\left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 2), \quad \left(\omega, \frac{\omega - 1}{\omega + 1}\right)$$

nur untereinander vertauscht zu werden,

2. für $q = 0$ nicht unendlich zu werden, so ist

$$\Phi_{a,c,\partial} = \text{constans}$$

eine Transformationsgleichung.

Um diese Bedingungen zu befriedigen, ist zunächst der Einfluß der Substitutionen (1) auf die Funktionen f zu untersuchen. Dieser ergibt sich aus den Zusammensetzungen § 69, (8) bis (13) und aus den Transformationsformeln für die f-Funktionen § 40.

Zur Abkürzung führen wir die Bezeichnung ein:

$$(3) \qquad \begin{aligned} f(\omega) &= u, & f\left(\frac{c + \partial\omega}{a}\right) &= v, \\ f_1(\omega) &= u_1, & \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\omega}{a}\right) &= v_1, \\ f_2(\omega) &= u_2, & \left(\frac{2}{\partial}\right) f_2\left(\frac{c + \partial\omega}{a}\right) &= v_2. \end{aligned}$$

Es ergeben sich dann folgende zusammengehörige Änderungen, wenn in der Bezeichnung auf die Verwandlung der Zahlen a, c, ∂ in a, c_1, ∂ oder a_2, c_2, ∂_2, wie sie eben durch die angeführten Formeln des § 69 charakterisiert ist, keine Rücksicht genommen wird:

$$
(4)\qquad
\begin{array}{cccc}
 & \omega, & u, & u_1, & u_2, \\
 & -\frac{1}{\omega}, & u, & u_2, & u_1, \\
 & \omega+1, & e^{-\frac{\pi i}{24}} u_1, & e^{-\frac{\pi i}{24}} u, & e^{\frac{\pi i}{12}} u_2, \\
 & \omega+2, & e^{-\frac{\pi i}{12}} u, & e^{-\frac{\pi i}{12}} u_1, & e^{\frac{\pi i}{6}} u_2, \\
\hline
\omega, & v, & & v_1, & v_2, \\
-\frac{1}{\omega}, & \varrho v, & & \varrho v_2, & \varrho v_1, \\
\omega+1, & \sigma e^{-\frac{n\pi i}{24}} v_1, & & \sigma e^{-\frac{n\pi i}{24}} v, & \sigma e^{\frac{n\pi i}{12}} v_2, \\
\omega+2, & \sigma^2 e^{-\frac{n\pi i}{12}} v, & & \sigma^2 e^{-\frac{n\pi i}{12}} v_1, & \sigma^2 e^{\frac{n\pi i}{6}} v_2,
\end{array}
$$

worin

$$\varrho = e^{-\frac{2\pi i}{3}[\alpha(\gamma-\beta)+(\alpha^2-1)\beta\delta]}, \qquad \sigma = \left(\frac{2}{a}\right) e^{\frac{(n-\lambda)\pi i}{24}}$$

zwei dritte Einheitswurzeln sind, die, falls n nicht durch 3 teilbar ist, den Wert 1 haben.

Um ferner die Wirkung der Substitution (2), die aus der Transformation zweiten Grades

$$\begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix}$$

hervorgeht, auf die Funktionen u, v zu ermitteln, müssen wir die Transformationen erster und $n$ter Ordnung

$$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}, \qquad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}$$

so bestimmen, daß

$$(5)\qquad \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}\begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}\begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix}\begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}$$

wird. Dieser Ansatz führt zu den Gleichungen

$$(6)\qquad \begin{array}{ll} a = a'(\alpha-\beta)+c'(\alpha+\beta), & a = \partial'(\alpha+\beta), \\ c-\partial = a'(\gamma-\delta)+c'(\gamma+\delta), & c+\partial = \partial'(\gamma+\delta). \end{array}$$

Hiermit ist zunächst, da $\alpha+\beta$ und $\gamma+\delta$ zufolge $\alpha\delta-\beta\gamma = 1$ relativ prim sind, ∂' bestimmt als der größte gemeinschaftliche Teiler von a und $c+\partial$, und aus $n = a'\partial'$ ergibt sich a'. Dann ist nach den Gleichungen (6):

$$\alpha+\beta = \frac{a}{\partial'}, \qquad \gamma+\delta = \frac{c+\partial}{\beta'},$$

und δ und β lassen sich so bestimmen, daß

$$(7) \qquad \delta(\alpha+\beta) - \beta(\gamma+\delta) = \alpha\delta - \beta\gamma = 1.$$

Aus den Gleichungen (6) für a und $c - \partial$ findet sich dann

$$(8) \qquad c' + a' = a\,\delta - (c - \partial)\beta.$$

δ und β können, da $\alpha+\beta$ und $\gamma+\delta$ beide ungerade sind, nach (7) nicht beide ungerade sein; folglich fällt c' nach (8) gerade aus. Ersetzt man, was nach (7) gestattet ist, δ, β durch $\delta + h\,(\gamma+\delta)$, $\beta + h\,(\alpha+\beta)$, für ein beliebiges h, so ändert sich c' nach (6) und (8) um $2ha'$, und über h kann so verfügt werden, daß c' durch 16 oder 48 teilbar wird.

Es ist dann nach (6) $\alpha+\beta+\gamma-\delta$ gerade und daher die Formel (12), § 40 anzuwenden. Darin ist nun zu berücksichtigen

$$\begin{matrix} a'(\alpha-\beta) \equiv a, & \partial(\alpha-\beta) \equiv \partial' \\ \partial'(\alpha+\beta) \equiv a, & a'(\gamma-\delta) \equiv -\partial \end{matrix} \pmod{16},$$

woraus folgt:

$$n(\alpha-\beta)(\alpha+\beta+\gamma-\delta) \equiv a^2 - \partial'^2 \pmod{16},$$

also

$$\left(\frac{2}{\alpha-\beta}\right) e^{-\frac{3\pi i}{8}(\alpha-\beta)(\alpha+\beta+\gamma-\delta)} = \left(\frac{2}{a}\right)\left(\frac{2}{a'}\right)\left(\frac{2}{a}\right)\left(\frac{2}{\partial'}\right) = \left(\frac{2}{n}\right)$$

und

$$\varrho = e^{-\frac{2\pi i}{3}[\alpha(\gamma-\beta)-(\alpha^2-1)\beta\delta]}.$$

Ist n nicht durch 3 teilbar, so ist

$$\begin{matrix} 2\alpha \equiv a(a'+\partial'), & 2\delta \equiv \partial(a'+\partial'), \\ 2\beta \equiv a(\partial'-a'), & 2\gamma \equiv \partial(\partial'-a') \end{matrix} \pmod{3},$$

also entweder α und δ oder β und γ durch 3 teilbar und also $\varrho = 1$.

Hieraus ergeben sich folgende zusammengehörige Vertauschungen (wobei die Änderung von a, c, ∂ in a', c', ∂' durch (6) bestimmt ist):

$$(9) \qquad \begin{matrix} \omega, & u, & v \\ \dfrac{\omega-1}{\omega+1}, & \dfrac{\sqrt{2}}{u}, & \varrho\left(\dfrac{2}{n}\right)\dfrac{\sqrt{2}}{v}. \end{matrix}$$

Wir wenden die Vertauschungen (4), (5), (9) auf folgende Funktionen an:

$$
(10) \qquad \begin{aligned} A &= \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r \\ B &= (uv)^s + \left(\frac{2}{n}\right)^{r+s} \frac{2^s}{(uv)^s}, \end{aligned}
$$

worin r, s zwei ganze Zahlen sind, die den Bedingungen

$$
(11) \qquad (n-1)r \equiv 0, \quad (n+1)s \equiv 0 \pmod{12}
$$

genügen, die also, wenn n durch 3 teilbar ist, beide durch 3 teilbar sind und

$$
\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}
$$

ist.

Es ergeben sich dann folgende zusammengehörige Vertauschungen:

$$
(12) \qquad \begin{array}{lll} \omega, & A, & B, \\ -\dfrac{1}{\omega}, & A, & B, \\ \omega + 2, & (-1)^{\frac{(n-1)r}{12}} A, & (-1)^{\frac{(n+1)s}{12}} B, \\ \dfrac{\omega - 1}{\omega + 1}, & \left(\dfrac{2}{n}\right)^r A, & \left(\dfrac{2}{n}\right)^r B. \end{array}
$$

Bilden wir nun aus A, B eine ganze rationale Funktion mit numerischen Koeffizienten

$$
(13) \qquad \Phi_{a,c,\mathfrak{d}} = \Sigma M_{h,k} A^h B^k,
$$

worin, falls in (12) Vorzeichenänderungen auftreten, die Exponenten h, k so einzurichten sind, daß in allen Gliedern von (13) die gleichen Vorzeichenveränderungen stattfinden, so wird das Funktionensystem $\Phi_{a,c,\mathfrak{d}}$ oder wenigstens $\Phi^2_{a,c,\mathfrak{d}}$ der Forderung 1. des oben aufgestellten Satzes genügen und wir haben, um auch die Forderung 2. zu befriedigen und so eine Transformationsgleichung zu erhalten, die Koeffizienten $M_{h,k}$ so zu bestimmen, daß die sämtlichen ν Werte von $\Phi_{a,c,\mathfrak{d}}$ für $q = 0$ endlich bleiben. Diese Aufgabe vereinfacht sich wesentlich, wenn n keinen quadratischen Teiler hat, und noch mehr, wenn n eine Primzahl ist.

Hat nämlich n keinen quadratischen Teiler, so kann man aus $\Phi_{a,0,\mathfrak{d}}$ die sämtlichen Werte $\Phi_{a,c,\mathfrak{d}}$ herleiten, durch Vermehrung von ω um gewisse ganze Zahlen; wenn also, was unsere Forderung ist, in der Entwickelung von $\Phi_{a,0,\mathfrak{d}}$ nach steigenden Potenzen von q keine negativen Potenzen vorkommen, so gilt das Gleiche von sämtlichen $\Phi_{a,c,\mathfrak{d}}$.

Ist aber n eine Primzahl, so genügt der Nachweis, daß $\Phi_{1,0,n}$ keine negativen Potenzen von q enthält, da das Gleiche durch Vertauschung von ω mit $\omega:n$ für $\Phi_{n,0,1}$ folgt.

Der konstante Wert, den die Funktion $\Phi_{a,c,b}$ erhält, bestimmt sich aus einem Gliede der Entwickelung.

Bei der Ausführung dieser Rechnungen dienen die Entwickelungen § 24, (11),

$$(14)\quad \begin{aligned} A &= q^{-\frac{n-1}{24}r} \prod_{1,\infty}^{h} \left(\frac{1+q^{n(2h-1)}}{1+q^{2h-1}}\right)^r \\ &\quad + q^{\frac{n-1}{24}r} \prod_{1,\infty}^{h} \left(\frac{1+q^{2h-1}}{1+q^{n(2h-1)}}\right)^r \\ B &= q^{-\frac{n+1}{24}s} \prod_{1,\infty}^{h} (1+q^{2h-1})^s (1+q^{n(2h-1)})^s \\ &\quad + \left(\frac{2}{n}\right)^{r+s} q^{\frac{(n+1)}{24}s} 2^s \prod_{1,\infty}^{h} \frac{1}{(1+q^{2h-1})^s (1+q^{n(2h-1)})^s}. \end{aligned}$$

Die Formeln werden nicht immer am einfachsten, wenn r, s möglichst klein angenommen werden, sondern es erweist sich am zweckmäßigsten, noch die Bedingung

$$(15)\quad \frac{(n-1)r}{12} \equiv \frac{(n+1)s}{12} \pmod 2$$

hinzuzufügen.

Wir erhalten so für die sieben ersten ungeraden Primzahlen folgende Bestimmung von A und B:

$$\begin{aligned} n &= 3, & A &= \left(\frac{u}{v}\right)^6 + \left(\frac{v}{u}\right)^6, & B &= (uv)^3 - \frac{8}{(uv)^3}, \\ n &= 5, & A &= \left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3, & B &= (uv)^2 - \frac{4}{(uv)^2}, \\ n &= 7, & A &= \left(\frac{u}{v}\right)^4 + \left(\frac{v}{u}\right)^4, & B &= (uv)^3 + \frac{8}{(uv)^3}, \\ n &= 11, & A &= \left(\frac{u}{v}\right)^6 + \left(\frac{v}{u}\right)^6, & B &= uv - \frac{2}{vu}, \\ n &= 13, & A &= \frac{u}{v} + \frac{v}{u}, & B &= (uv)^6 - \frac{64}{(uv)^6}, \\ n &= 17, & A &= \left(\frac{u}{v}\right)^3 + \left(\frac{v}{u}\right)^3, & B &= (uv)^4 + \frac{16}{(uv)^4}, \\ n &= 19, & A &= \left(\frac{u}{v}\right)^2 + \left(\frac{v}{u}\right)^2, & B &= (uv)^3 - \frac{8}{(uv)^3}. \end{aligned}$$

Die Entwickelungen nach Potenzen von q für A und B ergeben sich aus (14), soweit sie zur Rechnung gebraucht werden, folgendermaßen:

$$n = 3,\ A = q^{-\frac{1}{2}}(1 - 5q \ldots),$$
$$B = q^{-\frac{1}{2}}(1 - 5q \ldots),$$
$$n = 5,\ A = q^{-\frac{1}{2}}(1 - 2q \ldots),$$
$$B = q^{-\frac{1}{2}}(1 - 2q \ldots),$$
$$n = 7,\ A = q^{-1}\ (1 - 4q \ldots),$$
$$B = q^{-1}\ (1 + 3q \ldots),$$
$$n = 11,\ A = q^{-\frac{5}{2}}(1 - 6q + 21q^2 \ldots),$$
$$B = q^{-\frac{1}{2}}(1 - q + 2q^2 \ldots),$$
$$n = 13,\ A = q^{-\frac{1}{2}}(1 + 2q^2 - 2q^3 \ldots),$$
$$B = q^{-\frac{7}{2}}(1 + 6q + 15q^2 + 26q^3 \ldots),$$
$$n = 17,\ A = q^{-2}(1 - 3q + 6q^2 - 13q^3 + 25q^4 - 39q^5 + 76q^6 \ldots),$$
$$B = q^{-3}(1 + 4q + 6q^2 + 8q^3 + 17q^4 + 28q^5 + 54q^6 \ldots),$$
$$n = 19,\ A = q^{-\frac{3}{2}}(1 - 2q + 3q^2 - 5q^3 + 11q^4 - 13q^5 + 24q^6 - 28q^7 \ldots),$$
$$B = q^{-\frac{5}{2}}(1 + 3q + 3q^2 + 4q^3 + 9q^4 + 4q^5 + 39q^6 - 27q^7 \ldots),$$

und daraus erhält man durch Elimination der negativen Potenzen die gesuchten Gleichungen zwischen A und B:

$$\text{I.}\quad n = 3,\quad A - B = 0,$$
$$n = 5,\quad A - B = 0,$$
$$n = 7,\quad A - B + 7 = 0,$$
$$n = 11,\quad A - B^5 + B^3 + 2B = 0,$$
$$n = 13,\quad A^7 + 6A^5 + A^3 - 20A - B = 0,$$
$$n = 17,\quad A^3 - B^2 + 17AB - 34A^2 + 34B + 116A + 440 = 0,$$
$$n = 19,\quad A^5 - B^3 + 19AB^2 - 95A^2B + 109A^3 + 128B - 128A = 0\ ^{1)}.$$

[1]) Diese Gleichungen sind zuerst von **Schlaefli** aufgestellt (Journal für Mathematik, Bd. 72).

Aus diesem System von Gleichungen leitet man ein zweites und drittes her für die Funktionen f_1, f_2, indem man ω durch $\omega + 1$ und darauf ω durch $-1:\omega$ ersetzt. Diese beiden Systeme haben die gleiche Form, nur ist das eine Mal

$$u_1 = f_1(\omega), \quad v_1 = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\omega}{a}\right),$$

das andere Mal

$$u_1 = f_2(\omega), \quad v_1 = \left(\frac{2}{\partial}\right) f_2\left(\frac{c + \partial\omega}{a}\right)$$

zu setzen. Aus den Vertauschungen (4) ergibt sich so:

II. $n = 3,\quad A_1 = \left(\frac{u_1}{v_1}\right)^6 - \left(\frac{v_1}{u_1}\right)^6, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$

$A_1 + B_1 = 0,$

$n = 5,\quad A_1 = \left(\frac{u_1}{v_1}\right)^3 - \left(\frac{v_1}{u_1}\right)^3, \quad B_1 = (u_1 v_1)^2 + \frac{4}{(u_1 v_1)^2},$

$A_1 + B_1 = 0,$

$n = 7,\quad A_1 = \left(\frac{u_1}{v_1}\right)^4 + \left(\frac{v_1}{u_1}\right)^4, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$

$A_1 - B_1 - 7 = 0,$

$n = 11,\quad A_1 = \left(\frac{u_1}{v_1}\right)^6 - \left(\frac{v_1}{u_1}\right)^6, \quad B_1 = u_1 v_1 + \frac{2}{u_1 v_1},$

$A_1 + B_1^5 + B_1^3 - 2B_1 = 0,$

$n = 13,\quad A_1 = \frac{u_1}{v_1} - \frac{v_1}{u_1}, \quad B_1 = (u_1 v_1)^6 + \frac{64}{(u_1 v_1)^6},$

$A_1^7 - 6A_1^5 + A_1^3 + 20A_1 + B_1 = 0,$

$n = 17,\quad A_1 = \left(\frac{u_1}{v_1}\right)^3 + \left(\frac{v_1}{u_1}\right)^3, \quad B_1 = (u_1 v_1)^4 + \frac{16}{(u_1 v_1)^4},$

$A_1^3 - B_1^2 - 17A_1B_1 - 34A_1^2 - 34B_1 + 116A_1$
$+ 440 = 0,$

$n = 19,\quad A_1 = \left(\frac{u_1}{v_1}\right)^2 - \left(\frac{v_1}{u_1}\right)^2, \quad B_1 = (u_1 v_1)^3 + \frac{8}{(u_1 v_1)^3},$

$A_1^5 + B_1^3 - 19A_1B_1^2 + 95A_1^2B_1 - 109A_1^3$
$+ 128B_1 - 128A_1 = 0.$

§ 74. Die Form der Schlaeflischen Modulargleichungen für einen Primzahlgrad.

Die Form, die wir im vorigen Paragraphen für die zwischen

(1) $$u = f(\omega), \qquad v = f\left(\frac{c + \partial\,\omega}{a}\right)$$

bestehenden Relationen gefunden haben, läßt sich, wenigstens wenn der Transformationsgrad eine Primzahl p ist, leicht unter ein allgemeines Gesetz bringen. Da für die Folge viel auf diese Form ankommt, gehen wir hier noch etwas genauer darauf ein.

Die Bestimmung der Zahlen r, s nach (11) und (15) des vorigen Paragraphen hängt von dem Verhalten von p gegen den Modul 24 ab, und da wir den Fall $p = 3$ ausschließen können, so haben wir folgende Fälle:

(2)
$$\begin{array}{lll} p \equiv 1 \pmod{24} & r = 1 & s = 12 \\ p \equiv 5 & r = 3 & s = 2 \\ p \equiv 7 & r = 4 & s = 3 \\ p \equiv 11 & r = 6 & s = 1 \\ p \equiv 13 & r = 1 & s = 6 \\ p \equiv 17 & r = 3 & s = 4 \\ p \equiv 19 & r = 2 & s = 3 \\ p \equiv 23 & r = 12 & s = 1, \end{array}$$

so daß $r + s$ stets ungerade ist und $p + 1$ durch $2r$, $p - 1$ durch $2s$ teilbar ist. Hiernach wird

(3)
$$A = \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r,$$
$$B = (u\,v)^s + \left(\frac{2}{p}\right)\frac{2^s}{(u\,v)^s}.$$

Nun wissen wir, daß die $p + 1$ Größen v die Wurzeln einer irreducibeln Transformationsgleichung

(4) $$\Phi_p(v, u) = v^{p+1} + U_1 v^p + \cdots U_{p+1} = 0$$

sind, in der die Koeffizienten $U_1 \ldots, U_{p+1}$ rationale Funktionen von u sind.

Wir schließen sofort, daß es ganze rationale Funktionen von u sind. Denn erstens werden für $u = \infty$ die sämtlichen Wurzeln von (4) unendlich, wie man erkennt, wenn man $\omega = i\infty$, also $q = 0$ werden läßt. Zweitens geht nach (9) des vorigen

Paragraphen durch die Vertauschung $\left(u, \frac{\sqrt{2}}{u}\right)$ die Gesamtheit der Wurzeln v in

$$\left(\frac{2}{p}\right)\frac{\sqrt{2}}{v}$$

über. Hieraus folgt, daß für $u = 0$ die sämtlichen Wurzeln v in Null übergehen, also keine von ihnen unendlich wird, woraus zu schließen ist, daß nicht nur die $U_1, U_2, \ldots U_{p+1}$ ganze Funktionen von u sind, sondern daß auch jede von ihnen den Faktor u enthalten muß.

Wir schließen nun zunächst, genau wie bei der Invariantengleichung (§ 69, 2., 3. und 6.), daß

$$(5) \qquad \Phi_p(v, u) = \Phi_p(u, v),$$

und daß

$$(6) \qquad \Phi_p(v, u) = (v^p - u)(v - u^p) + p \sum_{1, p-1}^{h, k} c_{h, k} u^h v^k,$$

worin $c_{h,k} = c_{k,h}$ ganze Zahlen sind.

Wir wollen diese Funktion in der Weise darstellen

$$(7) \qquad \Phi_p(v, u) = v^{p+1} + u^{p+1} + \sum_{1, p}^{h, k} a_{h, k} u^h v^k,$$

worin also $a_{h,k} = a_{k,h}$ ebenfalls ganze Zahlen sind, auf deren Teilbarkeit durch p es nun weiter nicht ankommt, und es ist insbesondere $a_{p,p} = -1$. Wenn wir in der Gleichung

$$\Phi_p[f(p\omega), f(\omega)] = 0$$

ω durch $\omega + 2$ ersetzen, so ergibt sich wegen der Irreducibilität auf Grund der Relation

$$f(\omega + 2) = e^{-\frac{\pi i}{12}} f(\omega),$$

daß in (7) nicht alle Glieder, sondern nur solche vorkommen, in denen die Exponenten h, k der Kongruenz

$$(8) \qquad hp + k \equiv p + 1 \pmod{24}$$

genügen.

Nun kennen wir noch eine weitere Eigenschaft der Funktionen $\Phi_p(v, u)$, die sich aus der schon benutzten Vertauschung (9) des vorigen Paragraphen ergibt, wo $\varrho = 1$ zu setzen ist, und die, wenn wir zur Abkürzung

$$\varepsilon = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

setzen, so dargestellt werden kann:

(9) $$\Phi_p(v, u) = \left(\frac{uv}{\sqrt{2}}\right)^{p+1} \Phi_p\left(\frac{\varepsilon\sqrt{2}}{v}, \frac{\sqrt{2}}{u}\right).$$

Hieraus schließt man auf die Relationen

(10) $$\varepsilon^h\, 2^{\frac{h+k-p-1}{2}} a_{p+1-h,\, p+1-k} = a_{h,k}, \qquad a_{h,k} = a_{k,h}.$$

Wenn wir also in (7) die Glieder mit gleichen Koeffizienten $a_{h,k}$ zusammenfassen, so können wir uns auf die Annahme beschränken, daß $h \geqq k$, $h + k \geqq p + 1$ sei, und es ergibt sich Φ_p, von den beiden Gliedern v^{p+1}, u^{p+1} abgesehen, als ein Aggregat von Gliedern von den folgenden beiden Formen (wenn noch berücksichtigt wird, daß wegen (8) $\varepsilon^h = \varepsilon^k$ ist):

(11) $$v^h u^k + v^k u^h + \varepsilon^h\, 2^{\frac{h+k-p-1}{2}} (u^{p+1-h} v^{p+1-k} + u^{p+1-k} v^{p+1-h}) =$$
$$\underset{h > k}{(uv)^{\frac{p+1}{2}}} \left[\left(\frac{v}{u}\right)^{\frac{h-k}{2}} + \left(\frac{u}{v}\right)^{\frac{h-k}{2}}\right] \left[(uv)^{\frac{h+k-p-1}{2}} + \frac{\varepsilon^h\, 2^{\frac{h+k-p-1}{2}}}{(uv)^{\frac{h+k-p-1}{2}}}\right].$$

(12) $$v^h u^h + \varepsilon^h\, 2^{h - \frac{p+1}{2}} (uv)^{p+1-h}$$
$$= (uv)^{\frac{p+1}{2}} \left[(uv)^{h - \frac{p+1}{2}} + \frac{\varepsilon^h\, 2^{h-\frac{p+1}{2}}}{(uv)^{h-\frac{p+1}{2}}}\right].$$

Die Koeffizienten dieser Glieder in Φ_p sind ganze Zahlen.

Nun ergibt sich aus (8):
$$\left.\begin{array}{l}(h - k) \equiv (h - 1)(p + 1) \\ h + k - p - 1 \equiv -h(p - 1)\end{array}\right\} \pmod{24},$$
und daher ist $h - k$ durch $2r$, $h + k - p - 1$ (worin h auch $= k$ sein kann) durch $2s$ teilbar [§ 74, (2)].

Setzen wir daher
$$\frac{h-k}{2} = r\alpha, \quad \frac{h+k-p-1}{2} = s\beta,$$
so sind α und β positive ganze Zahlen, die zwischen den Grenzen

(13) $$0 \gtreqless \alpha < \frac{p+1}{2r}, \qquad 0 \gtreqless \beta \leqq \frac{p+1}{2s},$$

liegen, und überdies ergibt die aus (8) folgende Kongruenz $-h(p-1) \equiv 2s\beta \pmod{24}$, daß wenigstens in den Fällen, wo $\varepsilon = -1$ ist, $h \equiv \beta \pmod 2$ [§ 74, (2)], also stets $\varepsilon^h = \varepsilon^\beta$.

Demnach wird (11)

$$(uv)^{\frac{p+1}{2}}\left[\left(\frac{v}{u}\right)^{r\alpha}+\left(\frac{u}{v}\right)^{r\alpha}\right]\left[(uv)^{s\beta}+\frac{\varepsilon^{\beta}\,2^{s\beta}}{(uv)^{s\beta}}\right],$$

und (12)

$$(uv)^{\frac{p+1}{2}}\left[(uv)^{s\beta}+\frac{\varepsilon^{\beta}\,2^{s\beta}}{(uv)^{s\beta}}\right].$$

Nun gelten die bekannten Formeln, wenn x, γ beliebige Größen sind und

$$x+\frac{\gamma}{x}=y$$

gesetzt wird,

$$x^2+\frac{\gamma^2}{x^2}=y^2-2\gamma,\quad x^3+\frac{\gamma^3}{x^3}=y^3-3\gamma y,\ \ldots,$$

$$\left(x^n+\frac{\gamma^n}{x^n}\right)\left(x+\frac{\gamma}{x}\right)=x^{n+1}+\frac{\gamma^{n+1}}{x^{n+1}}+\gamma\left(x^{n-1}+\frac{\gamma^{n-1}}{x^{n-1}}\right),$$

woraus man durch den Schluß von n auf $n+1$ erkennt, daß

$$x^n+\frac{\gamma^n}{x^n}$$

sich für jedes beliebige n als ganze rationale Funktion $n$ten Grades von y darstellen läßt, die, wenn γ eine ganze Zahl ist, ganzzahlige Koeffizienten hat, deren höchster $=1$ ist.

Die beiden Größen

$$\left(\frac{v}{u}\right)^{r\alpha}+\left(\frac{u}{v}\right)^{r\alpha}\quad\text{und}\quad (uv)^{s\beta}+\frac{\varepsilon^{\beta}\,2^{s\beta}}{(uv)^{s\beta}}$$

können also in dieser Weise als ganze rationale Funktionen von A und B der Grade α und β dargestellt werden, und wir finden, wenn wir noch das dem Werte $\beta=\frac{p-1}{2s}$ entsprechende Glied, das den Koeffizienten -1 hat, absondern und mit $c_{\alpha,\beta}$ ganzzahlige Koeffizienten bezeichnen:

$$(14)\qquad \frac{\Phi_p(u,v)}{(uv)^{\frac{p+1}{2}}}=A^{\frac{p+1}{2r}}-B^{\frac{p-1}{2s}}+\sum^{\alpha,\beta} c_{\alpha,\beta}A^{\alpha}B^{\beta},$$

worin α und β an die Grenzen

$$0\leqq\alpha<\frac{p+1}{2r},\quad 0\leqq\beta<\frac{p-1}{2s}$$

gebunden sind. Dies ist die Form, die wir im vorigen Paragraphen den Modulargleichungen bis $p=19$ gegeben haben.

Es ist noch zu erwähnen, daß die in § 69, 4., 5. für die Invariantengleichung bei zusammengesetztem Transformationsgrade durchgeführte Betrachtung unverändert auch für die Schlaeflischen Modulargleichungen gilt, woraus wir schließen können, daß alle diese Gleichungen rationale Zahlenkoeffizienten haben.

§ 75. Die irrationalen Formen der Modulargleichungen.

Den Transformationsgleichungen lassen sich durch Anwendung desselben Verfahrens weit einfachere Formen geben. Die Gleichungsformen, mit denen wir uns jetzt beschäftigen werden, enthalten die drei Funktionen f, f_1, f_2 zugleich; da man aber nach § 34, (11), (12) zwei dieser Funktionen durch die dritte ausdrücken kann, so lassen sich zwei von ihnen eliminieren, und man kann so zu den Gleichungen des vorigen Paragraphen gelangen. Wenn man für f_1, f_2 die Ausdrücke durch f, oder für die drei Funktionen f, f_1, f_2 die Ausdrücke durch k^2 einsetzt, so kommen Wurzelzeichen vor, woraus sich der Name dieser Gleichungen erklärt.

Wir setzen wie oben

$$(1)\qquad \begin{aligned} u &= f(\omega), & v &= f\left(\frac{c+\partial\omega}{a}\right), \\ u_1 &= f_1(\omega), & v_1 &= \left(\frac{2}{a}\right) f_1\left(\frac{c+\partial\omega}{a}\right), \\ u_2 &= f_2(\omega), & v_2 &= \left(\frac{2}{\partial}\right) f_2\left(\frac{c+\partial\omega}{a}\right), \\ u u_1 u_2 &= \sqrt{2}, & v v_1 v_2 &= \left(\frac{2}{n}\right)\sqrt{2}, \end{aligned}$$

und erhalten folgende zusammengehörige Vertauschungen:

$$(2)\qquad \begin{array}{cccc} \omega, & u v, & u_1 v_1, & u_2 v_2, \\ -\dfrac{1}{\omega}, & \varrho u v, & \varrho u_2 v_2, & \varrho u_1 v_1, \\ \omega+1, & e^{-\frac{(n+1)\pi i}{24}} \sigma u_1 v_1, & e^{-\frac{(n+1)\pi i}{24}} \sigma u v, & e^{\frac{(n+1)\pi i}{12}} \sigma u_2 v_2, \end{array}$$

worin ϱ, σ die oben [§ 73, (4)] definierten dritten Einheitswurzeln sind.

Wir unterscheiden drei verschiedene Fälle nach dem Verhalten von n zum Modul 8.

1. $n + 1 \equiv 0$, (mod 8).

Wir setzen

$$2A = uv + (-1)^{\frac{n+1}{8}}(u_1 v_1 + u_2 v_2),$$

(3) $$B = uvu_1v_1 + uvu_2v_2 + (-1)^{\frac{n+1}{8}} u_1 v_1 u_2 v_2$$
$$= \frac{2}{u_1 v_1} + \frac{2}{u_2 v_2} + (-1)^{\frac{n+1}{8}} \frac{2}{uv},$$

so daß sich die zusammengehörigen Vertauschungen ergeben

(4) $$\begin{array}{ccc} \omega, & A, & B, \\ -\frac{1}{\omega}, & \varrho A, & \varrho^2 B, \\ \omega + 1, & e^{\frac{\pi i(n+1)}{12}} \sigma A, & e^{-\frac{\pi i(n+1)}{12}} \sigma^2 B. \end{array}$$

Ein Produkt von der Form $A^h B^k$ nimmt also durch die beiden Vertauschungen

$$\left(\omega, -\frac{1}{\omega}\right), \quad (\omega, \omega + 1)$$

die Faktoren an

$$\varrho^{h-k}, \quad e^{(h-k)\frac{(n+1)\pi i}{12}} \sigma^{h-k},$$

die $= 1$ sind, wenn $n + 1$ durch 3 teilbar ist. Wir bilden also jetzt mit numerischen Koeffizienten $M_{h,k}$ Funktionen der Form

(5) $$\Phi_{a,c,\mathfrak{d}} = \Sigma M_{h,k} A^h B^k,$$

worin, wenn $n \equiv 0$ oder $\equiv 1 \pmod 3$ ist, h und k nur solche (ganzzahlige) Werte annehmen dürfen, deren Differenzen $h - k$ bei der Teilung mit 3 denselben Rest lassen, wenn aber $n \equiv -1 \pmod 3$ dieser Beschränkung nicht unterworfen sind. Eine solche Funktion selbst, oder wenigstens ihre dritte Potenz genügt also einer Transformationsgleichung erster Stufe. Sie bleibt außerdem für alle endlichen Werte von $j(\omega)$ endlich und ist folglich eine ganze algebraische Funktion von $j(\omega)$. [Die Transformation zweiter Ordnung $\begin{pmatrix} 1, & 1 \\ -1, & 1 \end{pmatrix}$ braucht hier nicht zugezogen zu werden, da der Inbegriff der $\Phi_{a,c,\mathfrak{d}}$ schon bei der Substitution $(\omega, \omega + 1)$, nicht erst bei $(\omega, \omega + 2)$ ungeändert bleibt. Vgl. die Bemerkung am Anfang des § 73.]

Wenn wir also die Konstanten in $\Phi_{a,c,\mathfrak{d}}$ so bestimmen, daß in den Entwickelungen dieser Funktionen keine negativen Potenzen von q vorkommen, so müssen die sämtlichen $\Phi_{a,c,\mathfrak{d}}$ einer und derselben Konstanten gleich sein.

Zur Erreichung dieses Zieles genügt es auch hier, wenn n keinen quadratischen Teiler hat, daß $\Phi_{\alpha,0,\delta}$, und wenn n eine Primzahl ist, wenn $\Phi_{1,0,n}$ für $q = 0$ endlich bleibt.

Bei diesen Rechnungen machen wir Gebrauch von den Entwickelungen:

$$
(6)\qquad
\begin{aligned}
u v &= q^{-\frac{n+1}{24}} \Pi (1 + q^{n(2h+1)})(1 + q^{2h+1}),\\
u_1 v_1 &= q^{-\frac{n+1}{24}} \Pi (1 - q^{n(2h+1)})(1 - q^{2h+1}),\\
u_2 v_2 &= 2 q^{\frac{n+1}{12}} \Pi (1 + q^{2hn})(1 + q^{2h}),
\end{aligned}
$$

woraus durch Entwickelung nach Potenzen q:

$$
(7)\qquad
\begin{aligned}
u v &= q^{-\frac{n+1}{24}} (1 + q + q^3 + q^4 + q^5 + q^6 + q^7 + 2q^8 \ldots),\\
u_1 v_1 &= q^{-\frac{n+1}{24}} (1 - q - q^3 + q^4 - q^5 + q^6 - q^7 + 2q^8 \ldots),\\
u_2 v_2 &= 2 q^{\frac{n+1}{12}} (1 + q^2 + q^4 + 2q^6 + 2q^8 + \cdots).
\end{aligned}
$$

Die letzteren Formeln sind richtig für $n > 7$ (für $n = 3, 5, 7$ sind die Glieder von q^3, q^5, q^7 an zu modifizieren). Für $n = 7$, $n = 23$ zeigen diese Ausdrücke, daß A selbst für $q = 0$ endlich bleibt, woraus für diese Fälle die Gleichungen folgen:

$$
(8)\qquad
\begin{aligned}
n &= 7, & A &= 0,\\
n &= 23, & A &= 1.
\end{aligned}
$$

Durch einfache Rechnung findet man ferner noch:

$$
(9)\qquad
\begin{aligned}
n &= 31, & (A^2 - B)^2 - A &= 0,\\
n &= 47, & A^2 - A - B &= 2,\\
n &= 71, & A^3 - 4A^2 + 2A - B &= 1.
\end{aligned}
$$

Nicht ganz so einfach gestaltet sich die Rechnung für ein zusammengesetztes n. So muß man z. B. für $n = 15$ die Bedingung der Endlichkeit für $q = 0$ nicht nur für $\Phi_{1,0,15}$, sondern auch für $\Phi_{3,0,5}$ berücksichtigen. Diese beiden aber genügen. Man erhält so:

$$
(10)\qquad n = 15, \quad A^3 - AB + 1 = 0.
$$

2. Ist $n \equiv 3 \pmod 8$, so sind dieselben Schlüsse zu ziehen, wenn wir setzen:

$$
(11)\qquad
\begin{aligned}
4A &= u^2 v^2 - u_1^2 v_1^2 - u_2^2 v_2^2,\\
B &= u^2 v^2 u_1^2 v_1^2 + u^2 v^2 u_2^2 v_2^2 - u_1^2 v_1^2 u_2^2 v_2^2,
\end{aligned}
$$

für die man aus (2) die zusammengehörigen Vertauschungen erhält:

$$(12)\qquad \begin{array}{lll} \omega, & A, & B, \\ -\frac{1}{\omega}, & \varrho^2 A, & \varrho B, \\ \omega + 1, & e^{\frac{(n+1)\pi i}{6}} \sigma^2 A, & e^{-\frac{(n+1)\pi i}{6}} \sigma B, \end{array}$$

und hieraus leitet man in der gleichen Weise die Gleichungen ab:

$$(13)\qquad \begin{array}{ll} n = 3, & A = 0, \\ n = 11, & A = 1, \\ n = 19, & A^5 - 7A^2 - B = 0. \end{array}$$

3. Ist $n \equiv 1 \pmod 4$, so kann man ebenso verfahren mit den Funktionen

$$(14)\qquad \begin{aligned} 8A &= u^4 v^4 - u_1^4 v_1^4 - u_2^4 v_2^4 \\ B &= u^4 v^4 u_1^4 v_1^4 + u^4 v^4 u_2^4 v_2^4 - u_1^4 v_1^4 u_2^4 v_2^4, \end{aligned}$$

für die man die zusammengehörigen Vertauschungen erhält:

$$(15)\qquad \begin{array}{lll} \omega, & A, & B, \\ -\frac{1}{\omega}, & \varrho A, & \varrho^2 B, \\ \omega + 1, & e^{\frac{(n+1)\pi i}{3}} \sigma A, & e^{-\frac{(n+1)\pi i}{3}} \sigma^2 B. \end{array}$$

Nur der erste Fall $n = 5$ führt hier zu einem einfachen Resultat:

$$(16)\qquad n = 5, \quad A = 1.$$

Für $n = 5$ läßt sich noch eine einfachere Form der Transformationsgleichung gewinnen.

Wenn wir nämlich auf die drei Funktionen

$$(17)\qquad w = \frac{u_1^2 v_2^2 + u_2^2 v_1^2}{u\, v}, \quad w_1 = \frac{u_2^2 v^2 - v_2^2 u^2}{u_1 v_1}, \quad w_2 = \frac{u_1^2 v^2 - v_1^2 u}{u_2 v_2}$$

die Substitutionen $\left(\omega, -\frac{1}{\omega}\right)$, $(\omega, \omega + 1)$ anwenden, so ergeben sich unter der Voraussetzung $n \equiv 5 \pmod 8$ die zusammengehörigen Vertauschungen:

$$\begin{array}{llll} \omega, & w, & w_1, & w_2, \\ -\frac{1}{\omega}, & w, & w_2, & w_1, \\ \omega + 1, & e^{-\frac{\pi i}{24}(n-5)} w_1, & e^{-\frac{\pi i}{24}(n-5)} w, & e^{\frac{\pi i}{12}(n-5)} w_2. \end{array}$$

Setzt man also

$$A = w^2 + w_1^2 + w_2^2,$$
$$B = w^2 w_1^2 + w^2 w_2^2 + w_1^2 w_2^2,$$
$$C = w\, w_1 w_2,$$

so erhält man

$$\begin{array}{llll} \omega, & A, & B, & C, \\ -\frac{1}{\omega}, & A, & B, & C, \\ \omega + 1, & e^{-\frac{\pi i}{12}(n-5)} A, & e^{-\frac{\pi i}{6}(n-5)} B, & C, \end{array}$$

so daß zwei dieser Funktionen ebenso wie oben A und B benutzt werden können. Für $n = 5$ zeigt sich aber, daß in den Entwickelungen von w, w_1, w_2 nach Potenzen von q keine negativen Potenzen vorkommen und daß also A, B, C und mithin auch w, w_1, w_2 selbst konstant sind.

Es läßt sich also die Modulargleichung für $n = 5$ in jeder der drei Formen aufstellen:

$$\text{(18)} \qquad \begin{aligned} u_1^2 v_2^2 + u_2^2 v_1^2 &= 2\, u\, v, \\ u_2^2 v^2 - v_2^2 u^2 &= 2\, u_1 v_1, \\ u_1^2 v^2 - v_1^2 u^2 &= 2\, u_2 v_2. \end{aligned}$$

Diese Gleichungen lassen sich auch aus der von Jacobi (Fund. art. 30, gesammelte Werke, Bd. 1, S. 123) gegebenen herleiten.

Wir schließen diese Betrachtungen, indem wir in den einfachsten Fällen die Jacobischen Modulargleichungen aus diesen irrationalen Formen ableiten.

Wir setzen [vgl. § 54, (3)]:

$$\frac{u_2}{u} = x = \sqrt[4]{\varkappa}, \qquad \frac{u_1}{u} = x' = \sqrt[4]{\varkappa'},$$
$$\frac{v_2}{v} = y = \sqrt[4]{\lambda}, \qquad \frac{v_1}{v} = y' = \sqrt[4]{\lambda'},$$

und eliminieren mittels der Relationen

$$\text{(19)} \qquad \begin{aligned} x^8 + x'^8 &= 1, \quad x x' = \frac{\sqrt{2}}{u^3} \\ y^8 + y'^8 &= 1, \quad y y' = \frac{\sqrt{2}}{v^3} \end{aligned}$$

die Größen u und v.

Für $n = 3$ erhält man aus (13):

$$x^2 y^2 + x'^2 y'^2 = 1, \tag{20}$$

eine Form der Modulargleichung, die von Legendre herrührt.

Daraus, indem man für x', y' aus (19) die Werte setzt,

$$x^8 + y^8 = 4x^2y^2 - 6x^4y^4 + 4x^6y^6,$$

oder

$$(x^4 - y^4)^2 = 4(xy - x^3y^3)^2$$

und indem man hieraus die Wurzel zieht und das Vorzeichen durch $q = 0$ bestimmt, findet man:

$$x^4 - y^4 = 2xy - 2x^3y^3, \qquad (n = 3), \tag{21}$$

was, abgesehen von dem dort nicht näher erklärten Vorzeichen von $\sqrt[4]{\lambda}$, mit § 10, (12) übereinstimmt.

Für $n = 5$ folgt aus der zweiten Gleichung (18):

$$(x^2 - y^2)^3 = 4xyx'^4y'^4,$$

und daraus durch Quadrieren

$$(x^2 - y^2)^6 = 16x^2y^2(1 - x^8 - y^8 + x^8y^8),$$

was leicht in die Form gebracht wird

$$(x^2 - y^2)^2[(x^2 - y^2)^2 + 8x^2y^2]^2 = 16x^2y^2(1 - x^4y^4)^2.$$

Zieht man hieraus die Wurzel, so folgt, wie oben:

$$x^6 - y^6 - 4xy(1 - x^4y^4) + 5x^2y^2(x^2 - y^2) = 0 \quad (n = 5). \tag{22}$$

Für $n = 7$ erhält man, ohne Wurzelziehen, aus (8):

$$xy + x'y' = 1, \tag{23}$$

und daraus:

$$\begin{aligned} x^8 + y^8 - 8xy(1 + x^6y^6) + 28x^2y^2(1 + x^4y^4) \\ - 56x^3y^3(1 + x^2y^2) + 70x^4y^4 = 0 \qquad (n = 7). \end{aligned} \tag{24}$$

§ 76. Zusammengesetzte Transformationsgrade.

Ist der Transformationsgrad eine zusammengesetzte Zahl, so kann man noch einfachere Transformationsgleichungen aufstellen als die, die man auf dem Wege des vorigen Paragraphen gewinnt.

Wir führen diese Betrachtungen hier nur in den einfachsten Fällen durch.

Der ungerade Transformationsgrad n sei in zwei Faktoren zerlegt

$$n = n'n'', \tag{1}$$

die zueinander relativ prim sind.

Es lassen sich dann jeder Transformation n ten Grades von der Form

$$(2) \qquad \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}$$

je eine und nur eine Transformation der Grade n', n'':

$$(3) \qquad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \quad \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

zuordnen, die durch folgende Bedingungen bestimmt sind:

$$(4) \qquad \begin{aligned} a &= a'a'', & \partial &= \partial'\partial'', \\ \partial''c' &\equiv c \pmod{a'}, & \partial'c'' &\equiv c \pmod{a''}, \end{aligned}$$

und umgekehrt folgt aus jedem Paar Transformationen von der Form (3) nach (4) eine und nur eine Transformation (2). Nach (4) sind nämlich zunächst ∂', ∂'' bestimmt als die größten gemeinschaftlichen Teiler von ∂ mit n' und n'', und darauf wird c' nach dem Modul a', c'' nach dem Modul a'' bestimmt aus den beiden letzten Kongruenzen (4).

Es kommt nun vor allem darauf an, zu zeigen, daß die Kongruenzen (4) erhalten bleiben, wenn die Transformationen (2) und (3) nach § 69, (8) bis (12) durch die beiden linearen Transformationen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

umgeformt werden.

Wir setzen nach den erwähnten Formeln:

$$(5) \qquad \begin{aligned} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda, & 1 \end{pmatrix} \begin{pmatrix} a, & 0 \\ c_1, & \partial \end{pmatrix} \\ \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda', & 1 \end{pmatrix} \begin{pmatrix} a', & 0 \\ c_1', & \partial' \end{pmatrix} \\ \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} &= \begin{pmatrix} 1, & 0 \\ \lambda'', & 1 \end{pmatrix} \begin{pmatrix} a'', & 0 \\ c_2'', & \partial'' \end{pmatrix}. \end{aligned}$$

$$(6) \qquad \begin{aligned} \begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a_2, & 0 \\ c_2, & \partial_2 \end{pmatrix} \\ \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \begin{pmatrix} a_2', & 0 \\ c_2', & \partial_2' \end{pmatrix} \\ \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} &= \begin{pmatrix} \alpha'', & \beta'' \\ \gamma'', & \delta'' \end{pmatrix} \begin{pmatrix} a_2'', & 0 \\ c_2'', & \partial_2'' \end{pmatrix}. \end{aligned}$$

Es folgt zunächst aus § 69, (9):

$$c_1 \equiv c + \partial \pmod{a}, \quad c_1' \equiv c' + \partial' \pmod{a'}, \quad c_1'' \equiv c'' + \partial'' \pmod{a''},$$

woraus, nach (4)

$$\partial'' c_1' \equiv \partial'' c' + \partial \equiv c_1 \pmod{a'}$$
$$\partial' c_1'' \equiv \partial' c'' + \partial \equiv c_1 \pmod{a''}$$

in Übereinstimmung mit den Kongruenzen (4).

Für die Zusammensetzung (6) ergibt sich nach § 69, (12), daß ∂_2, ∂_2', ∂_2'' die größten gemeinschaftlichen Teiler von a, c; a', c'; a'', c'' sind; weil aber ∂'' relativ prim zu a', und $\partial'' c' \equiv c \pmod{a'}$ ist, so ist auch ∂_2' der größte gemeinschaftliche Teiler von a' und c und aus den gleichen Gründen ∂_2'' der größte gemeinschaftliche Teiler von a'' und c, woraus man schließt, da a', a'' relativ prim sind:

$$\partial_2 = \partial_2' \partial_2'', \quad a_2 = a_2' a_2''.$$

Ferner ist nach § 69, (11), (12), (13):

$$\partial_2 = \alpha c - \gamma a, \quad c_2 = -\partial \alpha,$$
$$\partial_2' = \alpha' c' - \gamma' a', \quad c_2' = -\partial' \alpha',$$

also nach (4):

$$\partial_2 c_2' - c_2 \partial_2' \equiv \alpha \alpha' (\partial c' - c \partial') \equiv 0 \pmod{n'},$$

folglich auch

$$\partial_2'' c_2' - c_2 \equiv 0 \pmod{a_2'},$$

in Übereinstimmung mit (4), und ebenso folgt:

$$\partial_2' c_2'' - c_2 \equiv 0 \pmod{a_2''},$$

wodurch also der Beweis geführt ist, daß die durch (4) ausgedrückte Zusammengehörigkeit der Transformationen

$$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}, \quad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \quad \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

durch Anwendung irgend einer linearen Transformation auf ω nicht gestört wird. Da wir hier n als ungerade voraussetzen, so können wir immer c, c', c'' durch 16 teilbar annehmen; und wenn n und folglich auch n', n'' durch 3 unteilbar sind, so können c, c', c'' auch durch 3 teilbar angenommen werden. Ist aber n durch 3 teilbar, so wird von den beiden Faktoren n', n'' der eine, etwa n'', durch 3 teilbar sein, der andere, n', nicht. Es kann dann c' noch durch 3 teilbar vorausgesetzt werden, nicht aber c und c''. In diesem Falle soll die Abhängigkeit des c'' von c noch näher bestimmt werden durch die Kongruenz

(7) $$\partial' c'' \equiv c \pmod{3a''}.$$

Eine Lösung dieser Kongruenz kann man immer aus einer Lösung der Kongruenz (4) $\partial' c'' \equiv c \pmod{a''}$ herleiten, indem man zu c'' ein Vielfaches von a'' hinzufügt.

Die Kongruenz (7) hat dann nach § 69, (9) bis (13) zur Folge:

$$\lambda \equiv n' \lambda'' \pmod{3}, \tag{8}$$

$$\begin{matrix} \alpha \equiv \alpha'' \partial' \partial_2', & \beta \equiv \beta'' a' \partial_2' \\ \gamma \equiv \gamma'' a' \partial_2', & \delta \equiv \delta'' \partial' \partial_2' \end{matrix} \pmod{3}. \tag{9}$$

Es mögen nun $v', v_1', v_2'; v'', v_1'', v_2''$ dieselbe Bedeutung für die Zahlen n', n'' haben, welche den v, v_1, v_2 in § 73, (3) für die Zahl n gegeben war, nämlich:

$$\begin{aligned} v' &= f\left(\frac{c' + \partial' \omega}{a'}\right), & v'' &= f\left(\frac{c'' + \partial'' \omega}{a''}\right), \\ v_1' &= \left(\frac{2}{a'}\right) f_1\left(\frac{c' + \partial' \omega}{a'}\right), & v_1'' &= \left(\frac{2}{a''}\right) f_1\left(\frac{c'' + \partial'' \omega}{a''}\right), \\ v_2' &= \left(\frac{2}{\partial'}\right) f_2\left(\frac{c' + \partial' \omega}{a'}\right), & v_2'' &= \left(\frac{2}{\partial''}\right) f_2\left(\frac{c'' + \partial'' \omega}{a''}\right). \end{aligned} \tag{10}$$

Wir wenden die Vertauschungstabelle (4), § 73 auf diese Funktionen an. Da n' unter allen Umständen durch 3 unteilbar ist, so sind die kubischen Einheitswurzeln $\varrho', \sigma' = 1$ zu setzen, während infolge der Kongruenzen (8), (9):

$$\varrho'' = \varrho^{n'}, \quad \sigma'' = \sigma^{n'} \tag{11}$$

wird. Wir erhalten hiernach folgende zusammengehörige Vertauschungen:

$$\begin{array}{llll} \omega, & v', & v_1', & v_2', \\ -\dfrac{1}{\omega}, & v', & v_2', & v_1', \\ \omega + 1, & e^{-\frac{n'\pi i}{24}} v_1', & e^{-\frac{n'\pi i}{24}} v', & e^{\frac{n'\pi i}{12}} v_2', \\ \hline \omega, & v'', & v_1'', & v_2'', \\ -\dfrac{1}{\omega}, & \varrho^{n'} v'', & \varrho^{n'} v_2'', & \varrho^{n'} v_1'', \\ \omega + 1, & \sigma^{n'} e^{-\frac{n''\pi i}{24}} v_1'', & \sigma^{n'} e^{-\frac{n''\pi i}{24}} v'', & \sigma^{n'} e^{\frac{n''\pi i}{12}} v_2'', \end{array} \tag{12}$$

die zusammen mit den Vertauschungen (4), § 73 gelten.

Wir unterscheiden jetzt zwei Fälle.

1. Wenn

$$(n' + 1)(n'' + 1) = 8\mu \equiv 0 \pmod{8} \tag{13}$$

ist, so setzen wir

$$(14)\qquad U = u v v' v'', \quad U_1 = u_1 v_1 v_1' v_1'', \quad U_2 = u_2 v_2 v_2' v_2'',$$

$$(15)\qquad \begin{aligned} 2A &= U + (-1)^\mu (U_1 + U_2), \\ B &= U U_1 + U U_2 + (-1)^\mu U_1 U_2, \\ &= \frac{4}{U_1} + \frac{4}{U_2} + (-1)^\mu \frac{4}{U}. \end{aligned}$$

Aus (12) und § 73, (4) erhalten wir dann folgende zusammengehörige Vertauschungen:

$$(16)\qquad \begin{array}{lll} \omega, & A, & B, \\ -\frac{1}{\omega}, & \varrho^{n'+1} A, & \varrho^{-(n'+1)} B, \\ \omega + 1, & \sigma^{n'+1} e^{\frac{2\mu\pi i}{3}} A, & \sigma^{-(n'+1)} e^{-\frac{2\mu\pi i}{3}} B. \end{array}$$

Wir wenden unser Prinzip zur Herleitung von Modulargleichungen auf diese Funktionen an und bemerken dazu noch folgendes:

Die in (16) vorkommenden dritten Einheitswurzeln sind $= 1$, wenn entweder n durch 3 unteilbar und μ durch 3 teilbar ist, oder n'' durch 3 teilbar ist und n' den Rest 2 läßt. In diesen Fällen ist jede rationale Funktion von A und B Wurzel einer Transformationsgleichung. In den anderen Fällen kommt diese Eigenschaft dem Kubus einer solchen rationalen Funktion von A und B zu, bei denen die Differenzen der Exponenten sämtlicher Glieder einander nach dem Modul 3 kongruent sind.

Sind diese rationalen Funktionen ganze Funktionen und sind außerdem ihre sämtlichen Werte für $q = 0$ endlich, so müssen sie einer Konstanten gleich sein, und dadurch gewinnen wir Transformationsgleichungen.

Sind n', n'' Primzahlen, so genügt es auch hier (vgl. § 72), wenn die negativen Potenzen von q in der Entwickelung einer solchen Funktion nach steigenden Potenzen von q in dem einen Hauptfall wegfallen, nämlich in dem, wo

$$\begin{pmatrix} a, & 0 \\ c, & \partial \end{pmatrix}, \quad \begin{pmatrix} a', & 0 \\ c', & \partial' \end{pmatrix}, \quad \begin{pmatrix} a'', & 0 \\ c'', & \partial'' \end{pmatrix}$$

gleich sind

$$\begin{pmatrix} 1, & 0 \\ 0, & n \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ 0, & n' \end{pmatrix}, \quad \begin{pmatrix} 1, & 0 \\ 0, & n'' \end{pmatrix},$$

also

$$U = f(\omega) f(n'\omega) f(n''\omega) f(n'n''\omega);$$

denn aus der Entwickelung für diesen einen Fall kann man die Entwickelungen für die übrigen Fälle herleiten, indem man ω ersetzt durch

$$(17) \qquad \frac{\omega}{n}, \quad \frac{\omega}{n'}, \quad \frac{\omega}{n''}$$

und dann noch ω um ganze Zahlen vermehrt, wodurch keine negativen Potenzen von q neu eingeführt werden können.

Für die Durchführung der Rechnung bedient man sich der Entwickelungen

$$(18) \qquad \begin{aligned} U &= q^{-\frac{(n'+1)(n''+1)}{24}} \times \\ &\Pi(1+q^{2h-1})(1+q^{(2h-1)n'})(1+q^{(2h-1)n''})(1+q^{(2h-1)n}) \\ U_1 &= q^{-\frac{(n'+1)(n''+1)}{24}} \times \\ &\Pi(1-q^{2h-1})(1-q^{(2h-1)n'})(1-q^{(2h-1)n''})(1-q^{(2h-1)n}) \\ U_2 &= 4\,q^{\frac{(n'+1)(n''+1)}{12}} \times \\ &\Pi(1+q^{2h})(1+q^{2hn'})(1+q^{2hn''})(1+q^{2hn}), \end{aligned}$$

die in den einzelnen Fällen die Potenzentwickelungen von A, B liefern, woraus die negativen Potenzen von q zu eliminieren sind. Man berechnet auf diese Weise sehr einfach die folgenden Gleichungen:

$$(19) \qquad \begin{aligned} n &= 15, \quad A = 1, \\ n &= 21, \quad (A^2 - B)^2 - A = 0, \\ n &= 33, \quad A^2 - B - A = 4, \\ n &= 35, \quad A^2 - B - A = 2, \\ n &= 55, \quad A^3 - B - 4A^2 - A + 4 = 0. \end{aligned}$$

2. Wenn

$$(n'-1)(n''-1) = 8\mu \equiv 0 \pmod 8,$$

so setzen wir

$$(20) \qquad \begin{aligned} A &= \frac{u\,v}{v'\,v''} + (-1)^\mu \left(\frac{u_1\,v_1}{v_1'\,v_1''} + \frac{u_2\,v_2}{v_2'\,v_2''}\right), \\ B &= \frac{v'\,v''}{u\,v} + (-1)^\mu \left(\frac{v_1'\,v_1''}{u_1\,v_1} + \frac{v_2'\,v_2''}{u_2\,v_2}\right), \end{aligned}$$

und erhalten nach (12) die zusammengehörigen Vertauschungen:

$$(21) \qquad \begin{array}{lll} \omega, & A, & B, \\ -\dfrac{1}{\omega}, & \varrho^{1-n'} A, & \varrho^{n'-1} B, \\ \omega + 1, & \sigma^{1-n'} e^{\frac{2\mu\pi i}{3}} A, & \sigma^{n'-1} e^{-\frac{2\mu\pi i}{3}} B. \end{array}$$

Wir können daher dasselbe Verfahren anwenden wie oben, wenn wir noch die Beschränkung hinzufügen, daß nur symmetrische Funktionen von A und B, d. h. rationale Funktionen von AB, $A+B$ benutzt werden, weil nur unter dieser Voraussetzung aus einem der Werte einer solchen Funktion durch die Vertauschungen (17) alle übrigen folgen. Man berechnet leicht die folgenden Beispiele:

$$\begin{aligned} n &= 15, \quad AB + 1 = 0, \\ n &= 35, \quad 2(A+B) - AB = 5 \\ n &= 39, \quad 2(A+B) - AB = 3. \end{aligned} \tag{22}$$

Die Rechnung bietet auch in noch komplizierteren Fällen keine unüberwindlichen Schwierigkeiten. So habe ich in der Abhandlung Acta mathematica Bd. II, S. 359 für den Fall $n = 105$ folgende Formel mitgeteilt:

$$A = \sum \frac{f(3\omega) f(5\omega) f(7\omega) f(105\omega)}{f(\omega) f(15\omega) f(21\omega) f(35\omega)},$$

$$B = \sum \frac{f(\omega) f(15\omega) f(21\omega) f(35\omega)}{f(3\omega) f(5\omega) f(7\omega) f(105\omega)},$$

$$\begin{aligned} A^2 + B^2 - 4(A+B)^3 + 10AB(A+B) \\ + 4(A+B)^2 + 10AB + 14(A+B) + 5 = 0, \end{aligned}$$

wenn sich die Summen Σ in A und B auf die drei Funktionen f, f_1, f_2 beziehen.

§ 77. Geometrische Deutung der irrationalen Modulargleichungen als Modularkorrespondenzen.

Den Inhalt der irrationalen Formen der Modulargleichungen machen wir durch eine geometrische Deutung anschaulicher. Betrachten wir zunächst den Fall $n \equiv -1 \pmod 8$ und setzen

$$x = f(\omega), \quad y = f_1(\omega), \quad z = f_2(\omega), \tag{1}$$

so wird hierdurch, wenn wir x, y, z als Cartesische Koordinaten eines Punktes P ansehen, eine Raumkurve dargestellt, die wir auch durch die beiden Gleichungen:

$$\begin{aligned} x^8 - y^8 - z^8 &= 0 \\ x\,y\,z &= \sqrt{2} \end{aligned} \tag{2}$$

ausdrücken können, und die wir die Grundkurve nennen wollen. Diese Kurve ist also von der 24. Ordnung. Man kann sie auf

eine ebene Kurve 3. Ordnung abbilden, wenn man $x^8 = X$, $y^8 = Y$ setzt:

(3) $$XY(X - Y) = 16.$$

Setzen wir [§ 75, (1)]

(4) $$\xi = f\left(\frac{c + \partial\omega}{a}\right), \quad \eta = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\omega}{a}\right), \quad \zeta = \left(\frac{2}{\partial}\right) f_2\left(\frac{c + \partial\omega}{a}\right),$$

so genüge die Größe ξ, η, ζ ebenfalls den Gleichungen (2), da $\left(\frac{2}{a}\right)\left(\frac{2}{\partial}\right) = \left(\frac{2}{n}\right) = +1$ ist, und der Punkt Π, dessen Koordinaten ξ, η, ζ sind, liegt also auch auf der Grundkurve.

Eine Gleichung

$$\Phi\,(x, y, z, \xi, \eta, \zeta) = 0$$

bedeutet, wenn der Punkt P festgehalten wird, eine Fläche, auf der Π liegen soll, und der Schnittpunkt dieser Fläche mit der Grundkurve gibt eine gewisse Anzahl von Punkten Π, die dem Punkt P entsprechen. Ebenso entspricht einem festen Punkt Π eine gewisse Anzahl von Punkten P, und diese Zuordnung heißt eine Korrespondenz auf der Grundkurve. Fällt der Punkt P mit einem der ihm entsprechenden Punkte Π zusammen, so erhalten wir einen Doppelpunkt oder Koinzidenz der Korrespondenz.

Wenn die Gleichung (5) bei Vertauschung von P mit Π sich nicht ändert, so ist die Korrespondenz eine wechselseitige. Solche Korrespondenzen sind durch die Gleichungen (8), (9), (10), § 75 gegeben.

Es ist dann nach § 75, (3)

(5) $$\begin{aligned} 2A &= x\xi + (-1)^{\frac{n+1}{8}}(y\eta + z\zeta) \\ B &= x\xi y\eta + x\xi z\zeta + (-1)^{\frac{n+1}{8}} y\eta z\zeta \end{aligned}$$

zu setzen. A ist vom ersten, B vom zweiten Grad in bezug auf die Koordinaten eines jeden der beiden Punkte P und Π.

Wir wollen den Grad von diesen Korrespondenzen, d. h. die Anzahl der einem Punkte P entsprechenden Punkte Π, feststellen. Dabei haben wir den Grad der Gleichung $\Phi = 0$ in bezug auf ξ, η, ζ mit dem Grad der Grundkurve, d. h. mit 24, zu multiplizieren und es ergibt sich:

für $n = 7$, $m = 24$,
„ $n = 23$, $m = 24$,
„ $n = 31$, $m = 96$,
„ $n = 47$, $m = 48$,
„ $n = 71$, $m = 72$,
„ $n = 15$, $m = 72$.

In den Fällen 23, 47, 71 ist also der Grad der Korrespondenz gleich dem Grad der entsprechenden Modulargleichung, d. h. gleich der Anzahl der betreffenden Transformationen; in den Fällen $n = 7, 31, 15$ ist der Grad das Dreifache des Grades der Modulargleichungen.

Was haben diese überzähligen Punkte zu bedeuten? Sie erklären sich dadurch, daß in diesen Fällen, in denen $n \equiv 0, 1 \pmod 3$ ist, in der Funktion $\Phi_{a,c,\partial}$ [§ 75, (5)], die nach der obigen Gleichung (5) einer Konstanten gleich ist, die Exponenten $h + 2k$ in allen Gliedern denselben Rest nach dem Modul 3 lassen, und daß also die Gleichung $\Phi = 0$ und ebenso die Gleichungen (2) erfüllt bleiben, wenn ξ, η, ζ mit einer beliebigen dritten Einheitswurzel multipliziert werden. Es geben also je drei Punkte der Korrespondenz dieselbe Transformation.

Wir hätten auch, wenn x, y, z durch (1) bestimmt sind, statt (4)

$$(6)\quad \xi = f\left(\frac{c + \partial\omega}{a}\right),\ \eta = \left(\frac{2}{\partial}\right) f_2\left(\frac{c + \partial\omega}{a}\right),\ \zeta = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\omega}{a}\right)$$

und folglich für A, B:

$$(7)\quad \begin{aligned} 2A &= x\xi + (-1)^{\frac{n+1}{8}}(y\zeta + z\xi), \\ B &= x\xi y\zeta + x\xi z\eta + (-1)^{\frac{n+1}{8}}\, y\eta z\zeta \end{aligned}$$

setzen können. Die Grundkurve und der Grad der Korrespondenz wären dann dieselben geblieben, aber die Koinzidenzen hätten eine andere, und zwar einfachere, Bedeutung bekommen. In beiden Fällen gehören die Koinzidenzen zu den singulären Werten der Modulfunktionen, in denen ω eine imaginäre quadratische Irrationalität ist, wie wir in der Folge noch genauer sehen werden.

Im Falle $n \equiv 3 \pmod 8$ setzen wir

$$(8)\quad \begin{gathered} x = f^2(\omega),\ y = f_1^2(\omega),\ z = f_2^2(\omega), \\ \xi = f^2\left(\frac{c + \partial\omega}{a}\right),\ \eta = f_1^2\left(\frac{c + \partial\omega}{a}\right),\ \varrho = f_2^2\left(\frac{c + \partial\omega}{a}\right), \end{gathered}$$

und erhalten eine Grundkurve

$$(9)\qquad \begin{aligned} x^4 - y^4 - z^4 &= 0, \\ x\,y\,z &= 2, \end{aligned}$$

die nur vom 12. Grade ist. Wir haben dann weiter nach § 75:

$$(10)\qquad \begin{aligned} 4A &= x\xi - y\eta - z\varrho, \\ B &= x\xi y\eta + x\xi z\varrho - y\eta z\varrho, \end{aligned}$$

und man erhält für den Grad m der Korrespondenz nach § 75 (13):

$$\begin{aligned} n &= 3, & m &= 12, \\ n &= 11, & m &= 12, \\ n &= 19, & m &= 60, \end{aligned}$$

also wieder wie im vorigen Falle, wenn $n \equiv 0, 1 \pmod 3$ ist, eine dreifach zu große Zahl.

Ist endlich $n \equiv 1 \pmod 4$, so setze man

$$x = f^4(\omega), \quad y = f_1^4(\omega), \quad z = f_2^4(\omega)$$

und erhält eine Grundkurve vom sechsten Grade.

Für $n = 5$ ergibt sich die richtige Zahl $m = 6$.

Achter Abschnitt.

Die Gruppe der Transformationsgleichungen und die Gleichung 5ten Grades.

§ 78. Die Galoissche Gruppe der Transformationsgleichungen für einen Primzahlgrad.

Ein eingehenderes algebraisches Studium der Transformationsgleichungen erfordert die Kenntnis ihrer Galoisschen Gruppe. Da wir die Transformationsgleichungen aus den Teilungsgleichungen hergeleitet haben, deren Gruppe uns bekannt ist (§ 63), so können wir die Gruppe der Transformationsgleichungen gleichfalls bilden.

Die Transformationsgleichungen ergaben sich (§ 65) dadurch, daß die Wurzeln der Teilungsgleichungen sich in Reihen einteilen ließen, die durch die Vertauschungen der Gruppe der Teilungsgleichung nicht auseinandergerissen, sondern nur untereinander vertauscht werden.

Jeder dieser Reihen ordnet sich eine bestimmte Wurzel einer Transformationsgleichung zu, und die Gruppe der letzteren besteht daher aus dem Inbegriff der Vertauschungen, die durch die Gruppe der Teilungsgleichung unter den Reihen hervorgerufen werden.

Ist der Transformationsgrad n eine ungerade Primzahl p, so gestattet diese Gruppe eine sehr elegante Darstellung, die zu weiteren Untersuchungen geeignet ist, und wir halten jetzt diese Voraussetzung fest.

Es wurde im § 65, (3) bereits die notwendige und hinreichende Bedingung ermittelt, daß zwei Wurzeln der Teilungsgleichung

(1) $$x_{\mu, \mu'}, \quad x_{\nu, \nu'}$$

in dieselbe Reihe R gehören, nämlich die Kongruenz

(2) $$\mu \nu' - \nu \mu' \equiv 0 \pmod{p}.$$

Wenn wir nun, wie es in der Zahlentheorie üblich ist (Gauss, Disquisitiones arithmeticae, art. 31), durch das Symbol

$$\frac{a}{b} \pmod{p}$$

eine ganze Zahl [oder Zahlklasse (mod p)] verstehen, die, mit b multipliziert, bei der Teilung durch p den Rest a läßt, so können wir, vorausgesetzt, daß μ' ν' nicht durch p teilbar sind, die eine Reihe definierende Kongruenz (2) auch so schreiben:

$$(3) \qquad \frac{\mu}{\mu'} \equiv \frac{\nu}{\nu'} \pmod{p},$$

und wir werden also naturgemäß darauf geführt, durch den Wert des Verhältnisses

$$(4) \qquad \frac{\mu}{\mu'} \equiv z \pmod{p},$$

das jeder der Zahlen $0, 1, \ldots, p-1$ kongruent sein kann, und das für eine ganze Reihe unveränderlich ist, diese Reihe R zu bezeichnen. Es bleibt dabei zunächst die eine Reihe unbezeichnet, in der μ' und folglich alle ν' durch p teilbar sind, aber auch diese Reihe ordnet sich der allgemeinen Bezeichnung sehr gut unter, wenn wir, falls $\mu' \equiv 0 \pmod{p}$

$$(5) \qquad \frac{\mu}{\mu'} \equiv \infty \pmod{p}$$

setzen, so daß wir also noch eine $(p+1)$te Reihe R_∞ erhalten. Die Gesamtheit der Reihen, deren Anzahl $p+1$ beträgt, ist hiernach zu bezeichnen durch

$$(6) \qquad R_\infty, R_0, R_1, \ldots, R_{p-1}.$$

Entsprechend werden die zugehörigen Wurzeln einer Transformationsgleichung mit

$$(7) \qquad v_\infty, v_0, v_1, \ldots, v_{p-1}$$

zu bezeichnen sein.

Wenn wir beispielsweise die Invariantengleichung (§ 69) zugrunde legen, so ist [nach den Bestimmungen des § 68, (10) über die Zahlen a, c, ∂]

$$(8) \qquad v_\infty = j(p\,\omega), \quad v_z = j\left(\frac{z+\omega}{p}\right)$$

zu setzen, und ebenso, wenn irgend eine andere Transformationsgleichung gewählt wird.

Nach dieser Bezeichnungsweise sind wir imstande, die Gruppe der Transformationsgleichung aus der der Teilungsgleichung sofort abzuleiten.

Wir setzen zunächst als Rationalitätsbereich den Inbegriff der rationalen Funktionen von $\varkappa^2$ mit rationalen Zahlenkoeffizienten fest.

Nach § 63, 3. besteht in diesem Rationalitätsbereich die Gruppe der Teilungsgleichung aus allen Substitutionen, durch die μ, μ' in

$$\begin{array}{c} \partial\mu - b\mu' \\ -c\mu + a\mu' \end{array}$$

übergeführt werden, worin a, b, c, ∂ beliebige, nach dem Modul p genommene ganze Zahlen sind, deren Determinante

$$\Delta = a\partial - bc \tag{9}$$

durch p nicht teilbar ist, und die Anzahl aller dieser Substitutionen beträgt

$$p(p-1)(p^2-1) \qquad [§ 63, (27)] \tag{10}$$

Daraus ergibt sich aber nach der Bezeichnungsweise (4), (5) die Gruppe der Transformationsgleichung als bestehend aus allen durch das Symbol

$$\left(z, \frac{\partial z - b}{-cz + a}\right) \pmod p \tag{11}$$

ausgedrückten Vertauschungen.

Wir bezeichnen eine Substitution (z, z'), wenn

$$z \equiv \frac{c + \partial z'}{a + bz'} \pmod p \tag{12}$$

ist, ähnlich wie früher durch

$$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \tag{13}$$

und erhalten für die Zusammensetzung zweier solcher Substitutionen, wenn

$$z' \equiv \frac{c' + \partial' z''}{a' + b' z''} \pmod p$$

ist, die Regel:

(14) $$(z, z')\,(z', z'')$$
$$\equiv \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} \equiv \begin{pmatrix} aa' + bc', & ab' + b\partial' \\ ca' + \partial c', & cb' + \partial\partial' \end{pmatrix} \pmod p,$$

in Übereinstimmung mit der Regel für die Zusammensetzung zweier Transformationen in § 28. Die Substitution (11) ist hiernach zu bezeichnen mit

$$\begin{pmatrix} \partial, & c \\ b, & a \end{pmatrix}.$$

Die durch alle Substitutionen dieser Form [nach (14)] gebildete Gruppe bezeichnen wir mit $\mathfrak{L}$ (Gruppe der linearen Substitutionen).

Die Funktionen (12) von z' und also auch die Substitutionen (13) bleiben ungeändert, wenn die vier Zahlen a, b, c, ∂ mit einem und demselben durch p nicht teilbaren Faktor multipliziert werden, und daraus ergibt sich nach (10) die Anzahl dieser Funktionen oder der Grad der Gruppe $\mathfrak{L}$

$$p\,(p^2 - 1), \tag{15}$$

den man auch leicht durch direkte Abzählung findet.

Werden in einer der Substitutionen (13) die vier Zahlen a, b, c, ∂ mit einem gemeinsamen, durch p unteilbaren Faktor multipliziert, so wird die Determinante Δ mit dem Quadrat dieses Faktors multipliziert. Es bleibt daher nicht die Determinante Δ, wohl aber ihr quadratischer Charakter, d. h. der Wert des Symbols

$$\left(\frac{\Delta}{p}\right)$$

durch diese Multiplikation erhalten.

Setzen wir zwei der Substitutionen (13) zusammen, so multiplizieren sich ihre Determinanten und hieraus folgt, daß alle Substitutionen der Gruppe $\mathfrak{L}$, in denen Δ quadratischer Rest von p ist, eine Gruppe unter sich bilden, die wir mit $\mathfrak{L}_0$ bezeichnen wollen.

Die Gruppe $\mathfrak{L}_0$ ist ein (eigentlicher) Divisor der Gruppe $\mathfrak{L}$ vom Index 2.

Setzt man die Substitutionen von $\mathfrak{L}_0$ zusammen mit irgend einer Substitution $(z, \beta z) = \begin{pmatrix} 1, & 0 \\ 0, & \beta^{-1} \end{pmatrix}$, wo β und also auch β^{-1} ein quadratischer Nichtrest von p ist, so erhält man die ganze Gruppe $\mathfrak{L}$.

Ist Δ quadratischer Rest von p, so kann man einen zu a, b, c, ∂ hinzuzufügenden gemeinsamen Faktor so wählen, daß $\Delta \equiv 1 \pmod{p}$ wird, so daß wir die Gruppe $\mathfrak{L}_0$ auch darstellen können durch

(16) $$\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod{p}.$$

In einer dieser Substitutionen sind die Zahlen α, β, γ, δ nach dem Modul p bis auf das gemeinsame Vorzeichen bestimmt. Der Grad der Gruppe $\mathfrak{L}_0$ ist

(17) $$\frac{1}{2} p (p^2 - 1).$$

Auf die Form (16) kommt man aber direkt, wenn man als die Gruppe der Teilungsgleichung nicht die Gruppe $\mathfrak{A}$, sondern die Gruppe $\mathfrak{B}$ des § 63 betrachtet, d. h. wenn man $p$te Einheitswurzeln dem Rationalitätsbereich adjungiert, woraus der Satz fließt:

Die Gruppe $\mathfrak{L}_0$ ist die Gruppe der Transformationsgleichung, wenn $p$te Einheitswurzeln dem Rationalitätsbereich adjungiert sind.

Zur Reduktion der Gruppe $\mathfrak{L}$ auf die Gruppe $\mathfrak{L}_0$ genügt aber schon die Adjunktion einer zweiwertigen Funktion und daher ist mit der Adjunktion der $p$ten Einheitswurzeln zu viel geschehen. Um zu erkennen, welche Irrationalität notwendig zu adjungieren ist, dienen die Sätze der §§ 63, 65.

Im § 63, 3. haben wir gesehen, daß die $p$te Einheitswurzel ϱ rational darstellbar ist durch die Wurzeln der Teilungsgleichung und daß durch eine Substitution der Gruppe $\mathfrak{A}$, deren Determinante mit m kongruent ist, ϱ in ϱ^m übergeht; ferner haben wir im § 65 nachgewiesen, daß durch Adjunktion sämtlicher Wurzeln einer Transformationsgleichung die Gruppe der Teilungsgleichung auf die Gruppe $\mathfrak{A}_0$ reduziert wird, die aus sämtlichen Substitutionen der Form

(18) $$\begin{pmatrix}a, 0\\ 0, a\end{pmatrix}.$$

besteht, wo a eine beliebige, durch p nicht teilbare Zahl ist. Die Determinanten der Substitutionen von $\mathfrak{A}_0$ sind also Quadrate und sind daher nach dem Modul p kongruent mit je einem der $\frac{1}{2}(p - 1)$ quadratischen Reste von p.

Die Summe

(19) $$A = \sum^{a} \varrho^{a},$$

worin für a die sämtlichen quadratischen Reste von p zu setzen sind, bleibt daher ungeändert durch die Substitutionen

von $\mathfrak{A}_0$ und ist infolgedessen rational durch die Wurzeln der Transformationsgleichung ausdrückbar. Die Summe A bleibt ungeändert durch die Substitutionen der Gruppe $\mathfrak{B}$ und also auch durch $\mathfrak{L}_0$, während sie durch die Substitutionen von $\mathfrak{A}$ und daher auch von $\mathfrak{L}$ zwei verschiedene Werte erhält, nämlich, wenn b die Reihe der Nichtreste durchläuft,

$$A = \overset{a}{\Sigma} \varrho^a, \qquad B = \overset{b}{\Sigma} \varrho^b.$$

A ist daher eine zur Gruppe $\mathfrak{L}_0$ gehörige Funktion und durch ihre Adjunktion wird $\mathfrak{L}$ auf $\mathfrak{L}_0$ reduziert.

Die Werte der Summen A, B sind aber bekannt (Bd. I, § 179):

$$A = \frac{-1 \pm \sqrt{(-1)^{\frac{p-1}{2}} p}}{2}, \quad B = \frac{-1 \mp \sqrt{(-1)^{\frac{p-1}{2}} p}}{2}.$$

Das Vorzeichen der Wurzel hängt von der Wahl der Wurzel ϱ ab und läßt sich bestimmen, kommt aber hier nicht in Betracht. Wir haben daher den Satz:

Die Gruppe der Transformationsgleichung ist $\mathfrak{L}_0$, wenn $\sqrt{(-1)^{\frac{p-1}{2}} p}$ dem Rationalitätsbereich adjungiert wird.

Die Gruppe der Invariantengleichung läßt sich auch ohne die Teilung der elliptischen Funktionen in folgender einfachen Weise ableiten, wobei man jedoch nur die Monodromiegruppe erhält, d. h. die Gruppe in dem Körper der rationalen Funktionen von $j(\omega)$, ohne Rücksicht auf die zu adjungierenden Konstanten. Wir beschränken uns auf den Fall eines Primzahlgrades p der Transformation, und setzen

$$(20) \qquad v_c = j\left(\frac{c+\omega}{p}\right), \quad v_\infty = j(p\omega), \quad u = j(\omega),$$

wobei c nach dem Modul p zu nehmen ist.

Wendet man auf ω eine lineare Substitution $S = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ an, so bleibt $j(\omega)$ ungeändert, und v_c geht in $v_{c'}$ über. Um c' zu finden, hat man eine zweite lineare Substitution $S' = \begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}$ zu suchen, so daß

$$\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}\begin{pmatrix}p, 0 \\ c', 1\end{pmatrix} = \begin{pmatrix}p, 0 \\ c, 1\end{pmatrix}\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$$

oder

$$\begin{aligned} p\alpha' + c'\beta' &= p\alpha, & \beta' &= p\beta \\ p\gamma' + c'\delta' &\equiv c\alpha + \gamma, & \delta' &= c\beta + \delta. \end{aligned}$$

Hieraus ergibt sich nach der dritten Gleichung: $c'\delta' \equiv c\alpha + \gamma$, und mit Hilfe der vierten:

$$c' \equiv \frac{c\alpha + \gamma}{c\beta + \delta} \pmod{p}.$$

Ist $c\beta + \delta \equiv 0$, so ergibt sich $c' \equiv \infty$, und ist $c \equiv \infty$, so folgt $c' \equiv \alpha/\beta$.

Bei der Anwendung auf die Bestimmung von c, c' kann man die $\alpha, \beta, \gamma, \delta$ durch kongruente Zahlen a, b, c, d ersetzen, deren Determinante $ad - bc$ quadratischer Rest von c ist, und es läßt sich auch zeigen, daß man auf diese Weise jede Substitution der Gruppe $\mathfrak{L}_0$ erhalten kann. Jede Funktion von v_c also, die durch die Substitutionen der Gruppe $\mathfrak{L}_0$ ungeändert bleibt, bleibt daher auch ungeändert, wenn auf ω eine lineare Substitution angewandt wird, und ist folglich eine rationale Funktion von $j(\omega)$. Wie aber die Koeffizienten in dieser Funktion beschaffen sind, darüber lehrt uns diese Betrachtung nichts, und es ist daher $\mathfrak{L}_0$ nur als die Monodromiegruppe der Invariantengleichung erkannt.

§ 79. Untersuchung der Gruppe $\mathfrak{L}_0$ [1]).

Wir haben im 10. Abschnitt des II. Bandes die Kongruenzgruppe und ihre Teiler ganz allgemein untersucht. Wir führen hier diese Untersuchung, soweit sie auf das Transformationsproblem Bezug hat, in spezieller Form noch einmal durch.

Die in $\mathfrak{L}_0$ enthaltenen Substitutionen

(1) $$\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix} = \left(z, \frac{-c + az}{\partial - bz}\right),$$

in denen

(2) $$\Delta = a\partial - bc$$

quadratischer Rest von p ist, können, wie schon oben bemerkt, auf die Form gebracht werden:

(3) $$\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} = \left(z, \frac{-\gamma + \alpha z}{\delta - \beta z}\right),$$

[1]) Über die Gruppe der linearen Substitutionen $\mathfrak{L}_0$ ist zu vergleichen: Galois, Liouvilles Journal, Bd. XI. Serret, Algèbre supérieure, Section IV, Chapitre IV. C. Jordan, Traité des Substitutions. Gierster, Gruppe der Modulargleichungen. Mathematische Annalen, Bd. 18.

worin

(4) $$\alpha\delta - \beta\gamma \equiv 1 \pmod{p},$$

wir haben nur, wenn wir unter $\sqrt{\Delta} \pmod{p}$ eine ganze Zahl verstehen, deren Quadrat nach dem Modul p kongruent mit Δ ist:

$$\begin{array}{ll} a \equiv \alpha\sqrt{\Delta}, & b \equiv \beta\sqrt{\Delta} \\ c \equiv \gamma\sqrt{\Delta}, & \partial \equiv \delta\sqrt{\Delta} \end{array} \pmod{p}$$

zu setzen. In der Form (3) können noch die Vorzeichen von α, β, γ, δ gleichzeitig geändert werden.

Wir fragen nach solchen Elementen z, die durch eine Substitution von der Form (3) ungeändert bleiben. Diese werden bestimmt durch die Kongruenz

$$z \equiv \frac{\gamma + \delta z}{\alpha + \beta z} \pmod{p},$$

oder

(5) $$\beta z^2 + (\alpha - \delta) z - \gamma \equiv 0 \pmod{p},$$

eine Kongruenz, die, wenn sie nicht identisch ist, höchstens zwei inkongruente Wurzeln hat. Um diese zu erhalten, schreiben wir, zunächst unter der Voraussetzung, daß β nicht durch p teilbar ist, die Kongruenz (5) so:

$$\left(\beta z + \frac{\alpha - \delta}{2}\right)^2 \equiv \left(\frac{\alpha - \delta}{2}\right)^2 + \beta\gamma \pmod{p},$$

oder mit Hilfe von (4):

(6) $$\left(\beta z + \frac{\alpha - \delta}{2}\right)^2 \equiv \left(\frac{\alpha + \delta}{2}\right)^2 - 1 \pmod{p}.$$

Demnach sind drei verschiedene Fälle zu unterscheiden:

I. $$\left(\frac{\alpha + \delta}{2}\right)^2 - 1 \equiv 0 \pmod{p};$$

dann hat die Kongruenz (5) eine Wurzel; es gibt ein und nur ein Element z, das ungeändert bleibt.

II. $\left(\frac{\alpha + \delta}{2}\right)^2 - 1$ quadratischer Rest von p;

die Kongruenz (5) hat zwei verschiedene Wurzeln, es gibt zwei Elemente z, die ungeändert bleiben.

III. $\left(\frac{\alpha + \delta}{2}\right)^2 - 1$ quadratischer Nichtrest von p;

die Kongruenz (5) hat gar keine Wurzel und alle Elemente z werden umgesetzt.

Ist $\beta \equiv 0$, so hat (5) immer die eine Wurzel $z = \infty$; ist dann $\delta \equiv \alpha$, und γ nicht $\equiv 0 \pmod{p}$, so gibt es nur diese eine; in diesem Falle ist aber

$$\alpha\delta \equiv 1, \quad \alpha \equiv \delta, \quad \left(\frac{\alpha+\delta}{2}\right)^2 \equiv 1 \pmod{p},$$

und die Bedingung I. erfüllt. Ist aber gleichzeitig $\gamma \equiv 0 \pmod{p}$, so ist die Substitution die identische.

Ist $\beta \equiv 0$, aber $\alpha - \delta$ nicht $\equiv 0 \pmod{p}$, so hat (5) noch eine zweite Wurzel; da jetzt $\alpha\delta \equiv 1 \pmod{p}$, so ist:

$$\left(\frac{\alpha+\delta}{2}\right)^2 - 1 \equiv \left(\frac{\alpha-\delta}{2}\right)^2 \pmod{p},$$

also quadratischer Rest, und die Bedingung II. erfüllt. Wir fassen diese Sätze so zusammen:

Im Falle I. bleibt ein Element oder alle Elemente ungeändert, im Falle II. bleiben zwei Elemente ungeändert und im Falle III. werden alle Elemente geändert.

Wenn wir eine und dieselbe Substitution

$$(7) \qquad A = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

mehrmals wiederholen, so entstehen die Substitutionen

$$A, A^2, A^3 \ldots,$$

in deren Reihe einmal die identische Substitution $\begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$ auftreten muß. Ist n die kleinste positive Zahl, für die

$$A^n = \begin{pmatrix} 1, & 0 \\ 0, & 1 \end{pmatrix}$$

ist, so heißt n der Grad von A (Bd. II, § 2).

Setzen wir für ein beliebiges m

$$A^m = \begin{pmatrix} \alpha_m, & \beta_m \\ \gamma_m, & \delta_m \end{pmatrix},$$

so erhalten wir zur Berechnung der Zahlen $\alpha_m, \beta_m, \gamma_m, \delta_m$ folgendes System rekurrenter Formeln:

$$(8) \qquad \begin{aligned} \alpha_{m+1} &= \alpha\alpha_m + \beta\gamma_m, & \beta_{m+1} &= \alpha\beta_m + \beta\delta_m, \\ \gamma_{m+1} &= \gamma\alpha_m + \delta\gamma_m, & \delta_{m+1} &= \gamma\beta_m + \delta\delta_m. \end{aligned}$$

Besonders einfach lassen sich hieraus die Zahlen $\alpha_m, \beta_m, \gamma_m, \delta_m$ im Falle I. berechnen.

In diesem Falle können wir, da die Vorzeichen von α, β, γ, δ alle gleichzeitig umgekehrt werden dürfen, annehmen:

$$\alpha + \delta \equiv 2, \quad \alpha\delta - \beta\gamma \equiv 1 \pmod{p},$$

und so erhalten wir aus (8):

$$\left.\begin{array}{ll} \alpha_2 \equiv -1 + 2\alpha, & \beta_2 \equiv 2\beta \\ \delta_2 \equiv -1 + 2\delta, & \gamma_2 \equiv 2\gamma \\ \alpha_3 \equiv -2 + 3\alpha, & \beta_3 \equiv 3\beta \\ \delta_3 \equiv -2 + 3\delta, & \gamma_3 \equiv 3\gamma \end{array}\right. \pmod{p},$$

woraus durch den Schluß von m auf $m+1$ gefolgert wird:

$$(9) \qquad \begin{array}{ll} \alpha_m \equiv -(m-1) + m\alpha, & \beta_m \equiv m\beta \\ \delta_m \equiv -(m-1) + m\delta, & \gamma_m \equiv m\gamma \end{array} \pmod{p}.$$

Hieraus ersieht man, daß die sämtlichen A^m wieder zum Falle I. gehören, und daß p der Grad von A ist.

Die analoge Betrachtung der beiden anderen Fälle ist von Serret durchgeführt, erscheint aber für unseren Zweck entbehrlich.

Dagegen wollen wir hier noch den Satz hinzufügen, daß die ganze Gruppe $\mathfrak{L}_0$ sich zusammensetzen läßt aus den beiden folgenden speziellen Substitutionen

$$(10) \qquad A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}.$$

Der Beweis ergibt sich aus § 30, wenn man beachtet, daß zu jedem der Bedingung $\alpha\delta - \beta\gamma \equiv 1 \pmod{p}$ genügenden Zahlensystem α, β, γ, δ sich das Zahlensystem α', β', γ', δ' so wählen läßt, daß

$$\begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} \equiv \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \pmod{p} \text{ und } \alpha'\delta' - \beta'\gamma' = 1$$

wird. Es sind also alle Substitutionen von $\mathfrak{L}_0$ unter den in § 30 betrachteten enthalten. Wir können hier aber auch leicht die Zusammensetzung einer beliebigen Substitution in $\mathfrak{L}_0$ aus A und B wirklich darstellen, und so unabhängig von § 30 den Beweis führen.

Denn wenn zunächst c eine beliebige, durch p nicht teilbare Zahl ist, so ergibt sich durch wirkliche Ausrechnung leicht

$$(11) \quad A^c = \begin{pmatrix} 1, & 0 \\ c, & 1 \end{pmatrix}, \quad C = \begin{pmatrix} c, & 0 \\ 0, & c^{-1} \end{pmatrix} = A^{-c^{-1}} B A^{-c} B A^{-c^{-1}} B,$$

und sodann, wenn $\begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$ eine beliebige Substitution in $\mathfrak{L}_0$ und β von 0 verschieden ist:

$$(12)\qquad \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} = \begin{pmatrix}1, & 0 \\ \delta\beta^{-1}, & 1\end{pmatrix} \begin{pmatrix}\beta, 0 \\ 0, \beta^{-1}\end{pmatrix} \begin{pmatrix}0, 1 \\ -1, 0\end{pmatrix} \begin{pmatrix}1, & 0 \\ \alpha\beta^{-1}, & 1\end{pmatrix},$$

und wenn $\beta = 0$ ist:

$$(13)\qquad \begin{pmatrix}\alpha, 0 \\ \gamma, \alpha^{-1}\end{pmatrix} = \begin{pmatrix}\alpha, 0 \\ 0, \alpha^{-1}\end{pmatrix} \begin{pmatrix}1, 0 \\ \gamma\alpha, 1\end{pmatrix}.$$

Es ist aus diesem Satz zu schließen, daß eine in $\mathfrak{L}_0$ enthaltene Gruppe, die die zwei Substitutionen A, B enthält, notwendig mit $\mathfrak{L}_0$ identisch sein muß.

§ 80. Normalteiler der Gruppe $\mathfrak{L}_0$.

Um die etwa möglichen Reduktionen der Transformationsgleichung kennen zu lernen, ist vor allem erforderlich, die Divisoren der Gruppe $\mathfrak{L}_0$ zu untersuchen. Wir fragen zuerst nach der Existenz eines Normalteilers $\mathfrak{K}$ von $\mathfrak{L}_0$ (Bd. II, § 3)[1]).

Ist

$$(1)\qquad S = \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix}$$

irgend eine von der identischen Substitution verschiedene Substitution in $\mathfrak{K}$, so ist, nach dem Wesen des Normalteilers, jede Substitution

$$(2)\qquad U = TST^{-1}$$

gleichfalls in $\mathfrak{K}$ enthalten, wenn

$$(3)\qquad T = \begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix}$$

eine beliebige Substitution in $\mathfrak{L}_0$ ist.

Wir stellen uns die Aufgabe, T und ξ so zu bestimmen, daß

$$(4)\qquad U = \begin{pmatrix}0, 1 \\ -1, \xi\end{pmatrix}$$

wird. Diese Bedingung kann auch so geschrieben werden:

$$\begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix} \begin{pmatrix}\alpha, \beta \\ \gamma, \delta\end{pmatrix} = \begin{pmatrix}0, 1 \\ -1, \xi\end{pmatrix} \begin{pmatrix}\alpha', \beta' \\ \gamma', \delta'\end{pmatrix},$$

[1]) Nach Galois: „Eigentliche Teiler".

und führt zu den Kongruenzen:

$$(5) \qquad \begin{array}{ll} 1. & \alpha'\alpha + \beta'\gamma \equiv \gamma' \\ 2. & \alpha'\beta + \beta'\delta \equiv \delta' \\ 3. & \gamma'\alpha + \delta'\gamma \equiv -\alpha' + \gamma'\xi \\ 4. & \gamma'\beta + \delta'\delta \equiv -\beta' + \delta'\xi \end{array} \pmod{p},$$

und aus 1. und 2. folgt noch:

$$(6) \qquad \begin{array}{ll} 5. & \alpha' \equiv \gamma'\delta - \delta'\gamma \\ 6. & \beta' \equiv -\gamma'\beta + \delta'\alpha \end{array} \pmod{p}.$$

Setzt man diese Werte in (5) 3. und 4. ein, so folgt:

$$\begin{array}{l} \gamma'(\alpha + \delta - \xi) \equiv 0 \\ \delta'(\alpha + \delta - \xi) \equiv 0 \end{array} \pmod{p},$$

woraus, da γ', δ' nicht beide durch p teilbar sein können, folgt:

$$(7) \qquad \xi \equiv \alpha + \delta \pmod{p};$$

ist ξ so bestimmt, so folgen in (5) die Kongruenzen 3., 4. aus 1., 2. Setzt man aber γ', δ' aus 1., 2. in

$$(8) \qquad \alpha'\delta' - \beta'\gamma' \equiv 1 \pmod{p}$$

ein, so erhält man

$$(9) \qquad \alpha'^2\beta + \alpha'\beta'(\delta - \alpha) - \beta'^2\gamma \equiv 1 \pmod{p}.$$

Ist hieraus α', β' bestimmt, so sind alle in (5), und also auch in (2), (4) ausgesprochenen Forderungen befriedigt.

Es handelt sich also noch darum, nachzuweisen, daß die Kongruenz (9) immer lösbar ist.

Diese Möglichkeit ist evident, wenn β oder $-\gamma$ quadratischer Rest von p ist; denn dann genügt

$$\begin{array}{lll} & \alpha' \equiv \sqrt{\beta^{-1}}, & \beta' \equiv 0 \\ \text{oder} & \alpha' \equiv 0, & \beta' \equiv \sqrt{-\gamma^{-1}} \end{array} \pmod{p}$$

der gestellten Forderung.

Im weiteren ist nun zu unterscheiden, ob die Substitution S zu Klasse I, II, III des vorigen Paragraphen gehört.

Ist zunächst

$$\text{I.} \qquad \left(\frac{\alpha + \delta}{2}\right)^2 \equiv 1 \pmod{p},$$

so geht, wenn wir S^m an Stelle von S setzen, nach § 79, (9), β in $m\beta$, γ in $m\gamma$ über, und es läßt sich m immer so bestimmen, daß $m\beta$ oder $-m\gamma$ quadratischer Rest von p wird.

Hierher gehört auch der Fall, daß $\beta \equiv 0$ oder $\gamma \equiv 0$ und $\alpha \equiv \delta \pmod{p}$ ist.

Ist dagegen $\beta \equiv 0$ und $\alpha - \delta$ nicht durch p teilbar, so kann man in (9) β' beliebig wählen und dann α' aus einer Kongruenz ersten Grades bestimmen.

Ist β nicht durch p teilbar, so setze man (9) in die Form

$$(10)\quad \left[\alpha'\beta + \beta'\left(\frac{\delta - \alpha}{2}\right)\right]^2 \equiv \beta + \beta'^2\left[\left(\frac{\alpha + \delta}{2}\right)^2 - 1\right] \pmod{p},$$

und wenn nun

II. $\left(\frac{\alpha + \delta}{2}\right)^2 - 1$ quadratischer Rest von p ist, so bestimme man β' aus der Kongruenz:

$$\beta'^2\left[\left(\frac{\alpha + \delta}{2}\right)^2 - 1\right] \equiv \left(\frac{\beta - 1}{2}\right)^2,$$

wodurch (10) übergeht in

$$\alpha'\beta + \beta'\left(\frac{\delta - \alpha}{2}\right) \equiv \pm \frac{\beta + 1}{2} \pmod{p},$$

und woraus α' bestimmt werden kann, welches Zeichen auch gewählt wird.

Ist

III. $\left(\frac{\alpha + \delta}{2}\right)^2 - 1$ quadratischer Nichtrest von p und zugleich β quadratischer Nichtrest, so läßt sich immer ein Nichtrest ν so bestimmen, daß $\beta + \nu$ quadratischer Rest wird; denn läßt man ν in $\beta + \nu$ die Reihe der Nichtreste durchlaufen, so können nicht lauter Nichtreste entstehen, weil unter diesen auch β sein müßte.

Dann kann man β' so bestimmen, daß

$$\beta'^2\left[\left(\frac{\alpha + \delta}{2}\right)^2 - 1\right] \equiv \nu \pmod{p},$$

und dann α' aus

$$\alpha'\beta + \beta'\left(\frac{\delta - \alpha}{2}\right) \equiv \pm\sqrt{\beta + \nu} \pmod{p}.$$

Hieraus folgt:

In einem Normalteiler $\mathfrak{K}$ der Gruppe $\mathfrak{L}_0$ muß gewiß eine Substitution U von der Form

$$(11)\qquad \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix}$$

vorkommen.

Es sei zunächst ξ von Null verschieden (mod p).

Nach dem Begriff des Normalteilers enthält $\mathfrak{K}$ auch die Substitution

$$(12) \qquad \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} \xi, & 1 \\ -1, & 0 \end{pmatrix}$$

und folglich auch

$$(13) \qquad \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} \begin{pmatrix} \xi, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ 2\,\xi, & 1 \end{pmatrix} \equiv A^{2\xi} \text{ [§ 79, (11)]},$$

also auch A und alle seine Potenzen. Daher enthält $\mathfrak{K}$ auch

$$(14) \qquad \begin{pmatrix} 1, & 0 \\ \eta, & 1 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & \xi \end{pmatrix} = \begin{pmatrix} 0, & 1 \\ -1, & \xi + \eta \end{pmatrix}$$

für ein beliebiges η, d. h. die Substitution (11) für jedes beliebige ξ und mithin auch

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}.$$

Demnach ist nach dem Satze des vorigen Paragraphen die Gruppe $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch.

Es bleibt noch die Möglichkeit zu erörtern, daß in (11) $\xi \equiv 0$ ist.

In diesem Falle enthält die Gruppe $\mathfrak{K}$ also die Substitution

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix},$$

und folglich auch für ein beliebiges, durch p nicht teilbares α

$$V = \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & 0 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} 0, & -\alpha \\ \alpha^{-1}, & 0 \end{pmatrix} \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} = \begin{pmatrix} \alpha^2, & 0 \\ 0, & \alpha^{-2} \end{pmatrix}.$$

Daraus leitet man, als in $\mathfrak{K}$ enthalten, noch weiter ab:

$$W = \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-2}, & 0 \\ 0, & \alpha^2 \end{pmatrix} \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} \begin{pmatrix} \alpha^2, & 0 \\ 0, & \alpha^{-2} \end{pmatrix} = \begin{pmatrix} 1, & 0 \\ \alpha^4 - 1, & 1 \end{pmatrix}.$$

Wenn nun p größer ist als 5, so kann man α so annehmen, daß $\alpha^4 - 1$ nicht durch p teilbar ist; dann enthält also $\mathfrak{K}$ auch die Substitution A und ihre Potenzen und mithin ist $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch.

Ist $p = 5$, so ist $\alpha^4 - 1$ immer durch p teilbar, also dieser Schluß nicht anwendbar.

In diesem Falle folgt aber aus dem Begriff des Normalteilers als in $\mathfrak{K}$ enthalten:

$$\begin{pmatrix}1, & 1\\ 2, & -2\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}-2, & -1\\ -2, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix}-2, & 0\\ 0, & 2\end{pmatrix},$$

$$\begin{pmatrix}-2, & 0\\ 0, & 2\end{pmatrix}\begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix}\begin{pmatrix}2, & 0\\ 0, & -2\end{pmatrix}\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix} = \begin{pmatrix}1, & 0\\ 2, & 1\end{pmatrix},$$

d. h. A^2 und mithin alle Potenzen von A, woraus wie oben zu schließen, daß $\mathfrak{K}$ mit $\mathfrak{L}_0$ identisch ist. Wir haben also den Satz:

Ist $p > 3$, so hat die Gruppe $\mathfrak{L}_0$ keinen Normalteiler.

Im Falle $p = 3$ enthält $\mathfrak{K}$ gleichfalls

$$\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix},$$

also auch

$$\begin{pmatrix}1, & 0\\ \pm 1, & 1\end{pmatrix}\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}\begin{pmatrix}1, & 0\\ \mp 1, & 1\end{pmatrix} = \begin{pmatrix}\mp 1, & 1\\ 1, & \pm 1\end{pmatrix},$$

und es bilden auch in der Tat die vier Substitutionen

(15) $$\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \quad \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}, \quad \begin{pmatrix}-1, & 1\\ 1, & 1\end{pmatrix}, \quad \begin{pmatrix}1, & 1\\ 1, & -1\end{pmatrix}$$

einen Normalteiler von $\mathfrak{L}_0$ im Index 3.

Im Falle $p = 3$ ist die Gruppe $\mathfrak{L}_0$ isomorph mit der alternierenden Gruppe der Vertauschungen von vier Elementen. Es ist dies die Gruppe einer beliebigen Gleichung vierten Grades, wenn die Quadratwurzel aus der Diskriminante dem Rationalitätsbereich adjungiert wird. Der Divisor (15) dieser Gruppe vom Index 3 liefert dann die in der Algebra bekannte kubische Resolvente der biquadratischen Gleichung.

Eine zur Gruppe (15) gehörige Funktion der Wurzeln v_∞, v_0, v_1, v_2 der Transformationsgleichung für den dritten Transformationsgrad ist z. B.

$$v_\infty v_0 + v_1 v_2$$

oder

$$(v_\infty - v_0)(v_1 - v_2).$$

Der Unterschied zwischen diesen beiden Funktionen ist der, daß die erstere durch die Substitution der Determinante -1

$$\begin{pmatrix}-1, & 0\\ 0, & 1\end{pmatrix}$$

ungeändert bleibt, während die zweite dabei ihr Zeichen ändert. Die erstere wird daher zu einer Gleichung dritten Grades mit rationalen Koeffizienten führen, während in der kubischen Gleichung für die zweite noch $\sqrt{-3}$ auftritt (§ 78).

§ 81. Nichtnormale Teiler von $\mathfrak{L}_0$.

Wir fragen nun, indem wir den Fall $p = 3$ beiseite lassen, nach den nichtnormalen Teilern der Gruppe $\mathfrak{L}_0$, deren Index kleiner als $p + 1$ ist; von der Existenz solcher Teiler hängt die Möglichkeit der Bildung von Resolventen der Transformationsgleichung ab, deren Grad niedriger ist als $p + 1$.

Zunächst läßt sich zeigen, daß der Index eines Teilers $\mathfrak{K}$ von $\mathfrak{L}_0$ niemals kleiner als p sein kann.

Es sei

$$\mathfrak{K} = S_0, S_1, \ldots, S_{\nu-1} \tag{1}$$

irgend ein Teiler von $\mathfrak{L}_0$ vom Grade ν, und, wenn es möglich ist,

$$T = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \tag{2}$$

eine Substitution $p$ten Grades, die in $\mathfrak{L}_0$, aber nicht in $\mathfrak{K}$ vorkommt. Es kann dann auch, da p Primzahl ist, keine niedrigere Potenz von T als die $p$te in $\mathfrak{K}$ vorkommen. Die Nebengruppen

$$\mathfrak{K}, \quad T\mathfrak{K}, \quad T^2\mathfrak{K}, \ldots, \quad T^{p-1}\mathfrak{K} \tag{3}$$

enthalten lauter voneinander verschiedene Elemente $T^i S_k$, und demnach ist νp höchstens gleich dem Grade der Gruppe $\mathfrak{L}_0$, d. h.:

$$\nu p \leqq p\,\frac{p^2-1}{2}.$$

Also ist der Index von $\mathfrak{K}$, d. h. der Quotient

$$p\,\frac{p^2-1}{2} : \nu$$

gleich p oder größer als p.

Ein Teiler $\mathfrak{K}$ von $\mathfrak{L}_0$, dessen Index kleiner als p ist, muß daher sämtliche Substitutionen $p$ten Grades enthalten, also auch (§ 79, I.) alle Substitutionen T, in denen

$$\alpha + \delta \equiv 2 \pmod{p} \tag{4}$$

ist.

Demnach enthält eine solche Gruppe $\mathfrak{K}$ zunächst die Substitution

$$A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix} \tag{5}$$

und ihre Potenzen; ebenso die Substitutionen

$$\begin{pmatrix}1, 2\\0, 1\end{pmatrix}, \quad \begin{pmatrix}2, 1\\-1, 0\end{pmatrix},$$

und folglich auch

(6) $$B = \begin{pmatrix}0, 1\\-1, 0\end{pmatrix} = \begin{pmatrix}1, 2\\0, 1\end{pmatrix}\begin{pmatrix}2, 1\\-1, 0\end{pmatrix}.$$

Wenn aber die Substitutionen A, B in $\mathfrak{K}$ enthalten sind, so muß $\mathfrak{K}$ nach § 79 mit $\mathfrak{L}_0$ identisch sein. Wir haben also den Satz:

Der Index eines Teilers von $\mathfrak{L}_0$ kann nicht kleiner als p sein.

Unser Problem beschränkt sich also auf die Frage nach den Teilern von $\mathfrak{L}_0$ vom Index p oder vom Grade $\frac{p^2-1}{2}$.

Es sei $\mathfrak{K}$ ein solcher Teiler und $S_0, S_1, \ldots, S_{\nu-1}$ seien seine Elemente, so daß die Zahl ν den Wert

(7) $$\nu = \frac{p^2-1}{2}$$

hat.

Da der Grad eines jeden Elementes einer Gruppe immer ein Teiler des Grades der Gruppe ist, so kann, da ν durch p nicht teilbar ist, in $\mathfrak{K}$ kein Element vom Grade p vorkommen; nehmen wir also für T die Substitution vom Grade p:

(8) $$A = \begin{pmatrix}1, 0\\1, 1\end{pmatrix},$$

so läßt sich die Gruppe $\mathfrak{L}_0$ in die p Nebengruppen zerlegen:

(9) $$\mathfrak{L}_0 = \mathfrak{K}, \quad A\mathfrak{K}, \quad A^2\mathfrak{K} \ldots, \quad A^{p-1}\mathfrak{K}.$$

Mit $\mathfrak{K}$ sind von demselben Grade, also auch von demselben Index alle seine konjugierten Teiler

$$T\mathfrak{K}T^{-1}.$$

Es sei nun g eine primitive Wurzel der Primzahl p, und

(10) $$C = \begin{pmatrix}g, 0\\0, g^{-1}\end{pmatrix},$$

eine Substitution, die offenbar vom Grade $\frac{p-1}{2}$ ist. Diese muß, wie jede Substitution von $\mathfrak{L}_0$, in einer der Reihen (9) vorkommen; d. h. es gibt eine Substitution S in $\mathfrak{K}$ und einen Exponenten λ, für den

(11) $$C = A^\lambda S, \quad S = A^{-\lambda} C.$$

Es läßt sich aber γ weiter so bestimmen, daß

(12) $$A^{\gamma-\lambda}CA^{-\gamma} = C,$$

man erhält dafür die Bedingung

$$\gamma(g - g^{-1}) \equiv \lambda g \pmod{p},$$

die, da $p > 3$ ist, immer befriedigt werden kann; danach ist aber wegen (11)

$$C = A^{\gamma}SA^{-\gamma}.$$

Es kommt also C in dem mit $\mathfrak{K}$ konjugierten Teiler $A^{\gamma}\mathfrak{K}A^{-\gamma}$ vor, und wir können also, indem diese Gruppe an Stelle von $\mathfrak{K}$ gesetzt wird, unbeschadet der Allgemeinheit annehmen, $\mathfrak{K}$ enthalte selbst die Substitution C.

Es kann nun in $\mathfrak{K}$ die Substitution

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$$

entweder vorkommen oder nicht vorkommen. Im ersten Fall enthält $\mathfrak{K}$ auch alle aus B und C zusammengesetzten Substitutionen, die sämtlich von einer der beiden Formen sind:

(13) $$\begin{pmatrix} g^r, & 0 \\ 0, & g^{-r} \end{pmatrix},$$

(14) $$\begin{pmatrix} 0, & g^{-r} \\ -g^r, & 0 \end{pmatrix}, \qquad r = 0, 1, \ldots \frac{p-3}{2},$$

und deren Anzahl $p - 1$ beträgt. Im ersten Fall enthält also $\mathfrak{K}$ alle Substitutionen von der Form (13), (14), im zweiten alle Substitutionen der Form (13) und **keine** der Form (14).

Es sei nun

(15) $$V = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$$

eine in $\mathfrak{K}$ enthaltene Substitution, die weder in der Form (13), noch in der Form (14) enthalten ist, bei der also weder α und δ, noch β und γ zugleich kongruent mit 0 sind. Dann sind die sämtlichen Substitutionen der Form

(16) $$C^r V C^s = \begin{pmatrix} \alpha g^{r+s}, & \beta g^{r-s} \\ \gamma g^{-r+s}, & \delta g^{-r-s} \end{pmatrix},$$

wenn r, s beide die Reihe der Zahlen durchlaufen:

$$0, 1, 2, \ldots \frac{p-3}{2}$$

in $\mathfrak{K}$ enthalten und alle **voneinander verschieden**. Denn sind zwei unter den Substitutionen (16) einander gleich, so muß

es auch eine unter ihnen geben, die, ohne daß r, s verschwinden, mit V identisch wird. Dies verlangt aber

$$\begin{matrix} \alpha \equiv \pm \alpha g^{r+s}, & \beta \equiv \pm \beta g^{r-s} \\ \gamma \equiv \pm \gamma g^{-r+s}, & \delta \equiv \pm \delta g^{-r-s} \end{matrix} \pmod{p},$$

wo in allen vier Formeln die oberen oder die unteren Zeichen gelten, also, da weder α und δ, noch β und γ gleichzeitig verschwinden,

$$r + s \equiv 0, \qquad r - s \equiv 0 \qquad \pmod{p-1},$$

oder

$$r + s \equiv \frac{p-1}{2}, \quad r - s \equiv \frac{p-1}{2} \qquad \pmod{p-1},$$

also in beiden Fällen

$$r \equiv 0, \quad s \equiv 0 \left(\bmod \frac{p-1}{2}\right), \qquad \text{w. z. b. w.}$$

In der Form (16) sind also $\left(\frac{p-1}{2}\right)^2$ verschiedene Substitutionen enthalten. Ist damit die Gruppe $\mathfrak{K}$ noch nicht erschöpft, so wähle man eine nicht in (13), (14), (16) enthaltene Substitution V' und bilde in gleicher Weise die Reihe

(17) $$C^r V' C^s,$$

deren Substitutionen sowohl unter sich als auch von den in (13), (14), (16) enthaltenen verschieden sind, und fahre auf diese Weise fort, bis die ganze Gruppe $\mathfrak{K}$ erschöpft ist.

Bezeichnen wir die Anzahl der so gebildeten Reihen (16), (17), ... mit q, so ergibt sich also der Grad der Gruppe $\mathfrak{K}$:

1. wenn B in $\mathfrak{K}$ nicht vorkommt:

$$= \frac{p-1}{2} + q \left(\frac{p-1}{2}\right)^2;$$

2. wenn B in $\mathfrak{K}$ vorkommt:

$$= p - 1 + q \left(\frac{p-1}{2}\right)^2,$$

und diese Zahl soll also nach der Forderung unserer Aufgabe

$$= \frac{(p-1)(p+1)}{2}$$

sein. Hieraus aber ergibt sich, daß der Fall 1. unmöglich ist, denn es müßte in diesem Falle

$$q \left(\frac{p-1}{2}\right) = p,$$

also
$$q = p, \quad p = 3$$
sein, was wir ausgeschlossen haben.

Im Falle 2. aber folgt für jedes beliebige p:
$$q = 2.$$

Daher muß in $\mathfrak{K}$ jedenfalls die Substitution B vorkommen, und die gesuchte Gruppe ist durch (13), (14), (16), (17) erschöpft.

Wir zeigen zunächst, daß in den beiden Substitutionen V, V' der Gruppe $\mathfrak{K}$ keine der Zahlen $\alpha, \beta, \gamma, \delta, \alpha', \beta', \gamma', \delta'$ kongruent 0 sein kann.

Es kommt nämlich, wie wir schon gesehen haben, in $\mathfrak{K}$ nicht vor
$$\begin{pmatrix} 1, & 0 \\ \gamma, & 1 \end{pmatrix},$$
wenn γ von 0 verschieden ist, also auch nicht
$$\begin{pmatrix} \alpha, & 0 \\ 0, & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 1, & 0 \\ \alpha\gamma, & 1 \end{pmatrix} = \begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix},$$
wenn α beliebig ist; und folglich auch nicht
$$\begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} = \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & \gamma \end{pmatrix}$$
$$\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix} \begin{pmatrix} \alpha, & 0 \\ \gamma, & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \gamma, & \alpha^{-1} \\ -\alpha, & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix} \begin{pmatrix} 0, & \alpha \\ -\alpha^{-1}, & -\gamma \end{pmatrix} = \begin{pmatrix} \alpha^{-1}, & \gamma \\ 0, & \alpha \end{pmatrix},$$
worin alle Substitutionen $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ enthalten sind, in denen eine der vier Zahlen $\alpha, \beta, \gamma, \delta$ kongruent mit 0 ist.

Die Substitutionen des Systems (16) bezeichnen wir jetzt mit
$$W = \begin{pmatrix} \alpha g^{r+s}, & \beta g^{r-s} \\ \gamma g^{-r+s}, & \delta g^{-r-s} \end{pmatrix},$$
und setzen

(18) $\xi \equiv \alpha g^{r+s}, \quad \varrho \equiv \alpha^{-1} \beta g^{-2s}$ (mod p).

(19) $\alpha\delta \equiv m, \quad \beta\gamma \equiv m - 1$

m ändert sich nicht, wenn V durch eine beliebige Substitution des Systems (16) ersetzt wird. Die Zahl m' soll die entsprechende Bedeutung für das System (17) haben; ξ kann in jedem dieser beiden Systeme jeden der Werte

(20) $1, 2, \ldots p - 1$

annehmen, und ϱ durchläuft, je nachdem $\alpha^{-1}\beta$ quadratischer Rest oder Nichtrest ist, in einem System die Reihe der Reste oder der Nichtreste. Die Änderung des Vorzeichens von ξ gibt keine neue Substitution W. Hiernach können wir W so darstellen:

$$W = \begin{pmatrix} \xi, & \xi\varrho \\ \xi^{-1}\varrho^{-1}(m-1), & \xi^{-1}m \end{pmatrix}. \tag{21}$$

Da nun das Quadrat von W

$$W^2 = \begin{pmatrix} \xi^2+m-1, & (\xi^2+m)\varrho \\ \xi^{-2}\varrho^{-1}(m-1)(\xi^2+m), & [(m-1)\xi^2+m^2]\xi^{-2} \end{pmatrix}$$

zu $\mathfrak{K}$ gehören muß, so ist es unter einem der Systeme (13), (14), (16), (17) enthalten, woraus sich folgende vier Möglichkeiten ergeben:

$$\begin{aligned} &1.\ \xi^2+m\equiv 0, \\ &2.\ \xi^2+m-1\equiv 0,\quad (m-1)\xi^2+m^2\equiv 0, \\ &3.\ (\xi^2+m-1)\,[(m-1)\xi^2+m^2]\equiv m\,\xi^2, \\ &4.\ (\xi^2+m-1)\,[(m-1)\xi^2+m^2]\equiv m'\,\xi^2, \end{aligned} \tag{22}$$

und jeder der $p-1$ Werte (20), für ξ gesetzt, muß einem dieser vier Fälle genügen. Wenn eine der Kongruenzen (22), 2. erfüllt ist, so muß die andere daraus folgen, was nur möglich ist, wenn

$$2m\equiv 1,\quad \xi^2\equiv m \pmod{p}. \tag{23}$$

Nun hat eine Kongruenz in bezug auf einen Primzahlmodul höchstens so viele inkongruente Wurzeln, als der Grad der Kongruenz beträgt; 1. und 2. können also höchstens für je zwei, 3. und 4. höchstens für je vier Werte von ξ befriedigt sein; also gibt es im ganzen höchstens zwölf Werte von ξ, die einer der vier Kongruenzen (22) genügen.

Daraus folgt:

$$p-1 \overline{\overline{<}}\, 12,\quad p \overline{\overline{<}}\, 13.$$

Ist aber $p=13$, so muß jede der Kongruenzen (22) die Maximalzahl von Wurzeln haben; es muß also auch 2. für zwei Werte von ξ befriedigt sein; dann müßte nach (23) $m\equiv 7$, $\xi^2\equiv 7 \pmod{13}$ sein, was unmöglich ist, da 7 quadratischer Nichtrest von 13 ist.

Ein Teiler von $\mathfrak{L}_0$ vom Index p existiert also nicht, wenn $p>11$ ist.

§ 82. Teiler von $\mathfrak{L}_0$ vom Index p für $p = 5, 7, 11$.

Es bleibt die Möglichkeit übrig, daß für $p = 5, 7, 11$ Teiler von $\mathfrak{L}_0$ vom Index p existieren.

1. $p = 5$. Wir untersuchen zunächst den Fall $p = 5$. Da m und $m - 1$ nicht kongruent 0 sein können, so bleiben für m die Annahmen

$$m \equiv 2, 3, 4 \pmod{p}.$$

Ersetzen wir aber die Substitution W § 81, (21) durch

$$(1) \qquad WB = \begin{pmatrix} -\xi \varrho, & \xi \\ -\xi^{-1} m, & \xi^{-1} \varrho^{-1} (m-1) \end{pmatrix},$$

wodurch m in $1 - m$ übergeht, so kommt der Fall $m \equiv 4$ auf den Fall $m \equiv 2$ zurück.

Für $m \equiv 2$ ist aber (23), § 81 nicht erfüllt, und von den Kongruenzen (22) ist keine möglich, da ± 2 Nichtreste von 5 sind und die linken Seiten von (22), 3., 4. sich für $m = 2$ auf $\xi^4 - 1$ reduzieren, was für jedes von Null verschiedene ξ durch 5 teilbar ist. Es bleibt also nur übrig, daß

$$(2) \qquad m \equiv 3, \quad m' \equiv 3 \pmod{5}$$

und die beiden Systeme W, W' [§ 81, (16), (17)] können sich nur dadurch voneinander unterscheiden, daß $\alpha^{-1}\beta$ und also auch ϱ in dem einen quadratischer Rest, in dem anderen quadratischer Nichtrest von 5 ist. Die gesuchte Gruppe besteht also, falls sie existiert, aus den 12 in den drei Formen

$$(3) \qquad \begin{pmatrix} \xi, & 0 \\ 0, & \xi^{-1} \end{pmatrix}, \quad \begin{pmatrix} 0, & \xi \\ -\xi^{-1}, & 0 \end{pmatrix}, \quad \begin{pmatrix} \xi, & \eta \\ 2\eta^{-1}, & 3\xi^{-1} \end{pmatrix}$$

enthaltenen Substitutionen, worin

$$\xi \equiv 1, 2, \quad \eta \equiv \pm 1, \pm 2 \pmod{5}$$

zu setzen ist.

2. $p = 7, 11$.

Da -1 für $p = 7, 11$ unter den quadratischen Nichtresten zu finden ist, so gehört die zusammengesetzte Substitution WB, (1), zu den W' [weil der quadratische Charakter der in (18), § 81 mit ϱ bezeichneten Größe in W und WB der entgegengesetzte ist]. Demnach ist nach (1) und § 81, (19), (21) $\beta'\gamma' \equiv -m \equiv m' - 1$, also:

$$(4) \qquad m + m' \equiv 1 \pmod{p}.$$

Für $p = 7$ bleiben also, da die Vertauschung von m mit m' nichts Neues liefert, die drei folgenden Möglichkeiten:

1. $m \equiv 2$, $m' \equiv 6$. 2. $m \equiv 3$, $m' \equiv 5$. 3. $m \equiv 4$, $m' \equiv 4$.

Im Falle 1. ist von den Kongruenzen § 81, (22), 1. und 2. unmöglich; also müßte für jedes ξ eine der beiden Kongruenzen 3., 4. erfüllt sein, die hier lauten:

$$(\xi^2 + 1)(\xi^2 + 4) \equiv 2\xi^2,\ 6\xi^2 \pmod 7,$$

deren keine für $\xi \equiv 1$ erfüllt ist.

Im Falle 3. ist (22), 1. nicht erfüllbar und (22), 2. ist für $\xi^2 \equiv 4$ erfüllt; daher muß für $\xi^2 \equiv 1, 2$ die Kongruenz (22) 3. oder 4.:

$$(\xi^2 + 3)(3\xi^2 + 2) \equiv 4\xi^2 \pmod 7$$

erfüllt sein, was wieder nicht der Fall ist. Es bleibt also für $p = 7$ allein übrig:

(5) $$m \equiv 3, \quad m' \equiv 5 \pmod 7.$$

Für $p = 11$ ist von vornherein die Möglichkeit auszuschließen, daß die Kongruenzen (22), 2. erfüllt seien, weil in diesem Falle infolge von (4) und § 81, (23):

$$m \equiv m'$$

sein müßte; dann wären (22), 3., 4. nicht verschieden und die Kongruenzen (22) könnten zusammen höchstens acht Wurzeln haben und nicht zehn, wie es doch sein müßte.

Es müssen also die Kongruenzen (22), 1., 3., 4 jede die Maximalzahl von Wurzeln haben, und es muß, damit 1. erfüllt sei, m, und aus gleichen Gründen m' quadratischer Nichtrest von 11 sein. Dieser Bedingung und gleichzeitig der Bedingung (4) genügen aber nur die beiden Zahlen

(6) $$m, m' \equiv 2, -1 \pmod{11}.$$

Die gesuchten Gruppen bestehen also in diesen beiden Fällen, falls sie existieren, aus folgenden Substitutionen:

$p = 7$

(7) $$\begin{pmatrix}\xi, 0\\ 0, \xi^{-1}\end{pmatrix}, \begin{pmatrix}0, \xi\\ \xi^{-1}, 0\end{pmatrix}, \begin{pmatrix}\xi & \xi\varrho\\ 2\xi^{-1}\varrho^{-1}, 3\xi^{-1}\end{pmatrix}, \begin{pmatrix}-\xi\varrho, & \xi\\ -3\xi^{-1}, & 2\xi^{-1}\varrho^{-1}\end{pmatrix}$$
$$\xi \equiv 1, 2, 3 \pmod 7,$$

$p = 11$

(8) $$\begin{pmatrix}\xi, 0\\ 0, \xi^{-1}\end{pmatrix}, \begin{pmatrix}0, & \xi\\ -\xi^{-1}, & 0\end{pmatrix}, \begin{pmatrix}\xi, & \xi\varrho\\ \xi^{-1}\varrho^{-1}, & 2\xi^{-1}\end{pmatrix}, \begin{pmatrix}-\xi\varrho, & \xi\\ -2\xi^{-1}, & \xi^{-1}\varrho^{-1}\end{pmatrix}$$
$$\xi \equiv 1, 2, 3, 4, 5 \pmod{11};$$

ϱ durchläuft in (7) und (8) entweder die Reihe der quadratischen Reste oder die der Nichtreste, so daß man für $p = 7$ oder 11 je zwei Gruppen vom Index p erhält.

Daß die in (3), (7), (8) zusammengestellten Substitutionssysteme wirklich Gruppen konstituieren, läßt sich durch direkte Zusammensetzung auf verschiedene Arten nachweisen. Einfacher gelangt man zu diesem Beweise aber dadurch, daß man Funktionen der v_z, § 78, (7), bildet, die durch die Substitutionen dieser Systeme ungeändert bleiben, und durch die Substitutionen von $\mathfrak{L}_0$ überhaupt nur p verschiedene Werte erhalten.

Die Systeme (3), (7), (8) lassen sich, wie aus ihrer Entstehungsweise hervorgeht, durch wiederholte Anwendung von B, C, U, U' zusammensetzen, wenn U, U' irgend zwei spezielle Substitutionen W, W' sind. Für $p = 5$ gehört U^2 und für $p = 7, 11$ gehört UB zu den W', so daß U' noch weggelassen werden kann. Wählen wir U irgendwie beliebig, und nehmen für die primitive Wurzel g in C für $p = 5, 7, 11$ bzw. $2, -2, 2$, so können wir die Gruppe (3) zusammensetzen aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 3 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & 1 \\ 2, & 3 \end{pmatrix} \qquad (p = 5),$$

die Gruppe (7) aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 4 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & \pm 1 \\ \pm 2, & 3 \end{pmatrix} \quad (p = 7),$$

die Gruppe (8) aus:

$$B = \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 2, & 0 \\ 0, & 6 \end{pmatrix}, \quad U = \begin{pmatrix} 1, & \pm 1 \\ \pm 1, & 2 \end{pmatrix} \quad (p = 11),$$

wo in den beiden letzten Fällen aus den doppelten Vorzeichen die oben erwähnten zwei verschiedenen Gruppen entspringen.

Wir stellen nun die diesen Substitutionen entsprechenden Vertauschungen der Indizes z zusammen [§ 79, (3)].

$p = 5$:

$$\begin{array}{rrrrrrl} z = \infty, & 0, & 1, & 2, & 3, & 4 & \\ 0, & \infty, & 4, & 2, & 3, & 1 & (B) \\ \infty, & 0, & 4, & 3, & 2, & 1 & (C) \\ 4, & 1, & 2, & 0, & \infty, & 3 & (U). \end{array}$$

Es werden also durch B, C, U die Indexpaare

$$(\infty, 0), \quad (1, 4), \quad (2, 3)$$

nicht auseinandergerissen, sondern nur untereinander vertauscht. Überdies werden jedesmal in zweien dieser Paare die Elemente vertauscht. Bilden wir daher eine Funktion wie

(9) $$V = (v_\infty - v_0)(v_1 - v_4)(v_2 - v_3),$$

so bleibt diese durch B, C, U und also durch das ganze System (3) ungeändert, während sie durch wiederholte Anwendung der zyklischen Vertauschung (0, 1, 2, 3, 4), d. h. der Substitution

$$A = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$$

fünf verschiedene Werte erhält. Aus A und B läßt sich aber [§ 79, (10)] die ganze Gruppe $\mathfrak{L}_0$ zusammensetzen, und V erhält daher durch Anwendung von $\mathfrak{L}_0$ nicht mehr als fünf Werte.

Die fünf Werte von V sind die Wurzeln einer Gleichung fünften Grades.

Für $p = 7$ ist

$$B = \left(z, -\frac{1}{z}\right), \quad C = (z, 4z), \quad U = \left(z, \frac{\mp 2 + z}{3 \mp z}\right).$$

Zur besseren Übersicht stellen wir noch B, C, U durch die zyklischen Vertauschungen dar, die durch sie in den acht Werten von z hervorgerufen werden:

$$B = (0, \infty)(1, -1)(2, 3)(-2, -3),$$
$$C = (1, -3, 2)(-1, 3, -2),$$
$$U = (\infty, \mp 1, \pm 1, \pm 3)(0, \mp 3, \mp 2, \pm 2),$$

und daraus erhält man die siebenwertige Funktion

(10) $$V = (v_\infty - v_0)(v_{\mp 1} - v_{\mp 3})(v_{\pm 1} - v_{\mp 2})(v_{\pm 3} - v_{\pm 2}),$$

worin das eine oder das andere Zeichen genommen werden kann.

Für $p = 11$ ist

$$B = \left(z, -\frac{1}{z}\right), \quad C = (z, 4z), \quad U = \left(z, \frac{\mp 1 + z}{2 \mp z}\right),$$

oder durch die Zyklen dargestellt:

$$B = (0, \infty)(1, -1)(2, 5)(-2, -5)(3, -4)(-3, 4),$$
$$C = (1, 4, 5, -2, 3)(-1, -4, -5, 2, -3),$$
$$U = (\infty, \mp 1, \pm 3, \mp 2, \pm 2)(0, \pm 5, \mp 5, \mp 4, \pm 1),$$

woraus die beiden 11wertigen Funktionen

(11) $$V = (v_\infty - v_0)(v_{\mp 1} - v_{\pm 5})(v_{\pm 3} - v_{\mp 5})(v_{\mp 2} - v_{\mp 4})(v_{\pm 2} - v_{\pm 1})(v_{\pm 4} - v_{\mp 3}).$$

Hierbei ist noch folgende Bemerkung von Interesse. Die Resolventen $p$ten Grades, deren Wurzeln die Größen (9), (10), (11) sind, enthalten nach § 78 in ihren Koeffizienten noch $\sqrt{\pm p}$.

Die Gruppe $\mathfrak{L}_0$ wird aber zur Gruppe $\mathfrak{L}$ erweitert, wenn wir eine lineare Substitution von der Form § 78, (13) hinzufügen, in der $a d - b c$ quadratischer Nichtrest ist, also etwa:

$$\begin{aligned} &\text{für } p = 5 \quad (z, 2z) \\ &\text{für } p = 7, 11 \quad (z, -z). \end{aligned}$$

Durch Anwendung dieser Substitution geht aber der Wert (9)

$$V = (v_\infty - v_0)(v_1 - v_4)(v_2 - v_3)$$

in den entgegengesetzten über, und daraus folgt, daß, wenn $p = 5$ ist, V^2 einer Gleichung 5ten Grades mit rationalen Zahlenkoeffizienten genügt. Daraus schließt man, daß in der Gleichung für V die Koeffizienten der ungeraden Potenzen den Faktor $\sqrt{5}$ haben, während die anderen rational sind, oder daß man für die Unbekannte $\sqrt{5}\, V$ eine Gleichung mit rationalen Koeffizienten erhält.

Für $p = 7, 11$ gehen die den beiden Vorzeichen in (10) oder (11) entsprechenden Ausdrücke durch die Vertauschung $(z, -z)$ ineinander über. Die Resolventen 7ten oder 11ten Grades, denen einer der beiden Ausdrücke (10) bzw. (11) genügt, gehen also durch Änderung des Vorzeichens von $\sqrt{-7}$, $\sqrt{-11}$ ineinander über.

§ 83. Verschiedene Resolventen 5ten Grades für den 5ten Transformationsgrad.

Bei der Bildung der Resolventen $p$ten Grades beschränken wir uns hier auf den Fall $p = 5$.

Diesen Resolventen kann man sehr mannigfaltige Formen geben, indem man nicht nur in der Funktion V, (9) des vorigen Paragraphen für die Größen v die Wurzeln einer beliebigen Transformationsgleichung wählen, sondern auch V durch mancherlei andere Funktionen ersetzen kann, etwa durch

$$(v_\infty + v_0)(v_1 + v_4)(v_2 + v_3),$$

oder durch

$$v_\infty v_0 + v_1 v_4 + v_2 v_3.$$

Wir wollen zunächst die Transformationsgleichung § 72, (8)' in der jetzt in Übereinstimmung mit dem vorigen Paragraphen v für x gesetzt ist:

(1) $$v^6 + 10 v^3 - \gamma_2 v + 5 = 0$$

anwenden. Hierin ist, wenn

$$c \equiv 0 \pmod{12}, \quad z \equiv c \pmod{5}$$

ist,

(2) $$v_\infty = 5 \left(\frac{\eta(5\omega)}{\eta \omega}\right)^2, \quad v_z = \left(\frac{\eta\left(\frac{\omega + c}{5}\right)}{\eta(\omega)}\right)^2.$$

Nehmen wir dann

(3) $$\begin{aligned} \sqrt{5}\, w_z &= (v_\infty - v_z)(v_{z+1} - v_{z-1})(v_{z-2} - v_{z+2}) \\ &= (v_\infty - v_c)(v_{c+12} - v_{c-12})(v_{c+24} - v_{c-24}), \\ z &= 0, 1, 2, 3, 4, \quad c = 0, \pm 12, \pm 24, \end{aligned}$$

so sind nach der Schlußbemerkung des vorigen Paragraphen die w_0, w_1, w_2, w_3, w_4 die Wurzeln einer Gleichung 5ten Grades, deren Koeffizienten rational aus γ_2 und rationalen Zahlen gebildet sind.

Beachtet man aber die Relationen [§ 54, (14)]:

$$\gamma_2(\omega + 1) = e^{-\frac{2\pi i}{3}} \gamma_2(\omega), \quad \gamma_2\left(-\frac{1}{\omega}\right) = \gamma_2(\omega),$$

so folgt aus der Form von (1), daß durch die Vertauschung $(\omega, \omega + 1)$ die Wurzeln v, abgesehen von einer Umstellung, den Faktor $e^{\frac{2\pi i}{3}}$ annehmen, während sie durch $\left(\omega, -\frac{1}{\omega}\right)$ ungeändert bleiben. Die w_z vertauschen sich also nur untereinander, und ihre symmetrischen Funktionen bleiben ungeändert und hängen daher rational nur von der Invariante $j(\omega)$ ab. Die Koeffizienten in der Gleichung für w können überdies für kein endliches $j(\omega)$ unendlich werden und sind demnach ganze Funktionen von $j(\omega)$.

Ein weiterer Aufschluß über diese Koeffizienten ergibt sich durch die Entwickelung nach steigenden Potenzen von q. Die Entwickelungen der v haben nach (2) die Anfänge

$$v_\infty = 5 q^{\frac{2}{3}} + \cdots, \quad v_z = e^{\frac{c}{12}\frac{2\pi i}{5}} q^{-\frac{2}{15}} + \cdots,$$

und daraus folgt mit Benutzung der bekannten Gleichung

$$4 \sin\frac{2\pi}{5} \cdot \sin\frac{4\pi}{5} = \sqrt{5}$$

der Anfang der Entwickelung für w_z:

(4) $$w_z = q^{-\frac{2}{5}} e^{\frac{c}{2}\frac{\pi i}{5}} + \cdots$$

Hieraus folgt, daß die Potenzsummen der w_z bis zur vierten einschließlich Konstanten sind, da sie nicht einmal die erste Potenz von $j(\omega)$ enthalten können, und daß das Produkt der w_z eine **lineare** Funktion von $j(w)$ sein muß, in der $j(\omega)$ den Koeffizienten 1 hat.

Die Gleichung der w hat daher die Form:

(5) $$w^5 + b_1 w^4 + b_2 w^3 + b_3 w^2 + b_4 w + b_5 = j(\omega),$$

wenn die b rationale Zahlen sind. Diese Koeffizienten lassen sich dadurch berechnen, daß man die Entwickelung (4) weiter fortsetzt. Wir schlagen hier einen anderen Weg ein, der, streng genommen, zu der im nächsten Teil behandelten komplexen Multiplikation gehört, bei seiner Einfachheit aber trotzdem ganz wohl hier seine Stelle finden kann.

Setzen wir $\omega = i = \sqrt{-1}$, so ist

$$\omega = -\frac{1}{\omega}$$

und infolgedessen ist [§ 34, (11), (12), (14)]:

$$f_1(i) = f_2(i) = \sqrt[8]{2}, \quad f(i) = \sqrt[4]{2},$$

also [§ 54, (5)]:

(6) $$\gamma_3(i) = 0, \quad \gamma_2(i) = 12, \quad j(i) = 12^3.$$

Man findet aber ferner aus den Transformationsformeln für $\eta(\omega)$ [§ 34, (4), (5)]:

$$\eta(\omega + 1) = e^{\frac{\pi i}{12}} \eta(\omega), \quad \eta\left(-\frac{1}{\omega}\right) = \sqrt{-i\omega}\, \eta(\omega),$$

wenn man auf die Zerlegung

$$5 = (2 + i)(2 - i)$$

Rücksicht nimmt:

$$\eta\left(\frac{12+i}{5}\right) = e^{\frac{\pi i}{6}} \eta\left(\frac{2+i}{5}\right) = e^{\frac{\pi i}{6}} \eta\left(\frac{1}{2-i}\right) = \sqrt{1+2i}\ \eta(i),$$

also

$$v_2 = 1 + 2i, \quad v_3 = 1 - 2i,$$

und man kann jetzt, da für $\gamma_2 = 12$ zwei Wurzeln der Gleichung (1) bekannt sind, für diesen besonderen Wert von γ_2 den linken Teil dieser Gleichung leicht in Faktoren zerlegen:

$$v^6 + 10v^3 - 12v + 5 = (v^2 + 2v + 5)(v^2 + v - 1)^2,$$

woraus zu schließen:

$$(7)\qquad \begin{aligned} v_\infty &= v_0 = \frac{-1+\sqrt{5}}{2}, \\ v_1 &= v_4 = \frac{-1-\sqrt{5}}{2}. \end{aligned}$$

(v_0, v_∞ müssen, da in ihnen q reell ist, positiv sein.)

Aus (3) ergibt sich sodann:

$$(8)\qquad \begin{aligned} w_0 = 0,\quad w_1 &= w_3 = -5 - 2i\sqrt{5}, \\ w_2 &= w_4 = -5 + 2i\sqrt{5}. \end{aligned}$$

Dies müssen die Wurzeln von (5) sein für $j = 12^3$ und daraus erhält man die gesuchte Resolvente in der Form:

$$(9)\qquad w(w^2 + 10w + 45)^2 = j(\omega) - 12^3 = \gamma_3^2.$$

Diese Gleichung läßt sich auch in die Form bringen:

$$(10)\qquad (w+3)^3(w^2 + 11w + 64) = j(\omega) = \gamma_2^3,$$

auf die man auch direkt kommt, wenn man, anstatt $\omega = i$ zu setzen,

$$\omega = \frac{-1 + i\sqrt{3}}{2}$$

annimmt.

Die gefundene Resolvente vereinfacht sich noch, wenn man [nach (9)]:

$$z = \sqrt{w} = \frac{\gamma_3}{w^2 + 10w + 45}$$

setzt:

$$(11)\qquad z^5 + 10z^3 + 45z = \gamma_3,$$

oder wenn man [nach (10)]

$$(12)\qquad w^2 + 11w + 64 = y^3,\quad y = \frac{\gamma_2}{w+3}$$

setzt:

$$(13)\qquad y^5 - 40y^2 - 5\gamma_2 y - \gamma_2^2 = 0,$$

eine Gleichung, die sich auch ergibt, wenn man von vornherein die Annahme macht:

$$2y = v_\infty v_0 + v_1 v_4 + v_2 v_3.$$

In der Gleichung (13) fehlen, wie man sieht, die dritte und die vierte Potenz der Unbekannten. Dieselbe Eigenschaft kommt auch, wie leicht nachzuweisen ist, der Gleichung zu, deren Wurzeln

(14) $$x = y(\lambda + \mu z) = \frac{(\lambda + \mu z)\gamma_2}{z^2 + 3}$$ [1])

sind, wenn λ, μ beliebige Parameter bedeuten, die für alle fünf Werte x die gleichen sind.

Setzt man diese Gleichung in die Form

(15) $$x^5 - 5ax^3 - 5b\gamma_2 x - bc\gamma_2^2 = 0,$$

so ergeben sich nach einigen Rechnungen mit Benutzung der besonderen Werte von x für $\gamma_3 = 0$ und $\gamma_3 = \infty$ für a, b, c die folgenden Ausdrücke:

(16) $$\begin{aligned} a &= 8\lambda^3 - 72\lambda\mu^2 + \gamma_3(\lambda^2\mu - \mu^3), \\ b &= \lambda^4 + 18\lambda^2\mu^2 - 27\mu^4 + \gamma_3\lambda\mu^3, \\ c &= \lambda^5 + 10\lambda^3\mu^2 + 45\lambda\mu^3 + \gamma_3\mu^5. \end{aligned}$$

Es soll noch eine Resolvente 5ten Grades mit Benutzung der Funktion $f(\omega)$ gebildet werden.

Wir setzen:

(17) $$u = f(\omega), \quad v_\infty = f(5\omega), \quad v_z = f\left(\frac{\omega + c}{5}\right)$$
$$c \equiv 0 \pmod{48}, \quad z \equiv c \pmod{5},$$

und haben nach § 73 zwischen u und v die Gleichung 6ten Grades:

(18) $$u^6 + v^6 - u^5v^5 + 4uv = 0.$$

Wir untersuchen den Einfluß, den die drei Vertauschungen

$$(\omega, \omega + 2), \quad \left(\omega, -\frac{1}{\omega}\right), \quad \left(\omega, \frac{\omega - 1}{\omega + 1}\right)$$

auf die Größen v_z haben. Durch diese Vertauschungen geht c über in c_1, c_2, c', die nach § 69, (9), (11) und § 73, (6) durch die Kongruenzen

(19) $$c_1 \equiv c + 2, \quad c_2 \equiv -\frac{1}{c}, \quad c' \equiv \frac{c - 1}{c + 1} \pmod{5}$$

bestimmt sind. Abgesehen von dieser Änderung des Index gehen nach § 73, (4) und (9) die v über in

(20) $$e^{-\frac{5\pi i}{12}}v, \quad v, \quad -\frac{\sqrt{2}}{v}.$$

---

[1]) Vgl. Kiepert, Auflösung der Gleichung 5ten Grades. Crelles Journal, Bd. 87, S. 114.

Man hat also, wenn zur Abkürzung $e^{-\frac{5\pi i}{12}} = \varepsilon$ gesetzt wird, folgende zusammengehörige Vertauschungen:

$$
(21)\quad \begin{array}{cccccccc}
\omega, & u, & v_\infty, & v_0, & v_1, & v_2, & v_3, & v_4, \\
\omega + 2, & e^{-\frac{\pi i}{12}} u, & \varepsilon v_\infty, & \varepsilon v_2, & \varepsilon v_3, & \varepsilon v_4, & \varepsilon v_0, & \varepsilon v_1; \\
-\frac{1}{\omega}, & u, & v_0, & v_\infty, & v_4, & v_2, & v_3, & v_1, \\
\frac{\omega - 1}{\omega + 1}, & \frac{\sqrt{2}}{u}, & -\frac{\sqrt{2}}{v_1}, & -\frac{\sqrt{2}}{v_4}, & -\frac{\sqrt{2}}{v_0}, & -\frac{\sqrt{2}}{v_2}, & -\frac{\sqrt{2}}{v_3}, & -\frac{\sqrt{2}}{v_\infty}.
\end{array}
$$

Wir führen nun die fünf Größen w_z durch die Gleichung ein:

$$
(22)\qquad w_z = \frac{(v_\infty - v_z)(v_{z+1} - v_{z-1})(v_{z+2} - v_{z-2})}{\sqrt{5}\, u^3},
$$

also:

$$
w_0 = \frac{(v_\infty - v_0)(v_1 - v_4)(v_2 - v_3)}{\sqrt{5}\, u^3},
$$

$$
w_1 = \frac{(v_\infty - v_1)(v_2 - v_0)(v_3 - v_4)}{\sqrt{5}\, u^3},
$$

$$
w_2 = \frac{(v_\infty - v_2)(v_3 - v_1)(v_4 - v_0)}{\sqrt{5}\, u^3},
$$

$$
w_3 = \frac{(v_\infty - v_3)(v_4 - v_2)(v_0 - v_1)}{\sqrt{5}\, u^3},
$$

$$
w_4 = \frac{(v_\infty - v_4)(v_0 - v_3)(v_1 - v_2)}{\sqrt{5}\, u^3},
$$

so daß, wenn man in der letzten Reihe davon Gebrauch macht, daß nach (18) das Produkt der sechs Größen v_z den Wert u^6 hat, sich aus (21) folgende zusammengehörige Vertauschungen der w ergeben:

$$
(23)\quad \begin{array}{cccccc}
\omega, & w_0, & w_1, & w_2, & w_3, & w_4, \\
\omega + 2, & -w_2, & -w_3, & -w_4, & -w_0, & -w_1, \\
-\frac{1}{\omega}, & w_0, & w_2, & w_1, & w_4, & w_3, \\
\frac{\omega - 1}{\omega + 1}, & -w_0, & -w_3, & -w_4, & -w_2, & -w_1.
\end{array}
$$

Die Funktionen w können für keinen von 0 und ∞ verschiedenen Wert von u unendlich werden. Nehmen wir daher die Gleichung, deren Wurzeln die fünf Größen w_z sind, in der Form an:

$$
w^5 + A_1 w^4 + A_2 w^3 + A_3 w^2 + A_4 w + A_5 = 0,
$$

so sind A_1^2, A_2, A_3^2, A_4, A_5^2 nach den Grundsätzen des § 73 ganze rationale Funktionen von

$$u^{24} + \frac{2^{12}}{u^{24}}. \tag{24}$$

Die Entwickelung von (24) nach steigenden Potenzen von q fängt an mit q^{-1}, während der Anfang der Entwickelung von w_z

$$q^{-\frac{1}{10}} e^{-\frac{c\pi i}{60}}$$

ist. Die Größen A_1^2, A_2, A_3^3, A_4 können daher nicht einmal die erste Potenz von (24) enthalten und sind also konstant, während A_5^2 die Form hat:

$$A_5^2 = u^{24} + \frac{2^{12}}{u_{24}} + C,$$

worin C eine Konstante ist. Die Werte der Konstanten kann man bestimmen, wenn man die Werte der w_z für $\omega = i$ kennt. Es ist aber für $\omega = i$ [vgl. oben (6), (7)]:

$$u = f(i) = \sqrt[4]{2},$$
$$v_3 = f\left(\frac{i+48}{5}\right) = f\left(\frac{i-2}{5} + 10\right) = e^{-\frac{10\pi i}{24}} f\left(\frac{i-2}{5}\right),$$
$$= e^{-\frac{10\pi i}{24}} f(i+2) = -i\sqrt[4]{2},$$
$$v_2 = i\sqrt[4]{2}$$

und folglich nach (18):

$$v_\infty = v_0 = \sqrt[4]{2}\,\frac{1+\sqrt{5}}{2},$$
$$v_1 = v_4 = \sqrt[4]{2}\,\frac{1+\sqrt{5}}{2}.$$

Folglich wird:

$$w_0 = 0, \quad w_1 = w_2 = i\sqrt{5}, \quad w_3 = w_4 = -i\sqrt{5}.$$

Danach wird zunächst $C = -2^7$, also

$$A_5^2 = \left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

und daraus durch Vergleichung der Anfänge der Entwickelung

$$A_5 = -u^{12} + \frac{64}{u^{12}},$$

und die Gleichung für w bekommt die Form:

$$w(w^2 + 5)^2 = u^{12} - \frac{64}{u^{12}}. \tag{25}$$

Man kann ihr aber noch eine andere, sehr bemerkenswerte Form geben.

Nach den zwischen den Funktionen $f(\omega)$, $f_1(\omega)$, $f_2(\omega)$ bestehenden Relationen [§ 34, (11), (12)] ist:

$$\frac{f(\omega)^{24} - 64}{f(\omega)^{12}} = \frac{[f_1(\omega)^8 - f_2(\omega)^8]^2}{f(\omega)^4}.$$

Führen wir also für w die neue Unbekannte

(26) $$y = \sqrt{w} = \frac{f_1(\omega)^8 - f_2(\omega)^8}{f(\omega)^2 (w^2 + 5)}$$

ein, so erhalten wir die Form:

(27) $$y^5 + 5y = \frac{f_1(\omega)^8 - f_2(\omega)^8}{f(\omega)^2}.$$

Auf diese Formeln gründet sich die von **Hermite** und **Kronecker** geschaffene Auflösung der Gleichung fünften Grades durch elliptische Funktionen, auf die wir im 14. Abschnitt des II. Bandes hingewiesen haben.

Nach Bd. I, § 60 kann die allgemeine Gleichung fünften Grades auf die Form reduziert werden:

(28) $$z^5 + 5z = a,$$

und diese Gleichung wird mit (27) identisch, wenn man setzt:

$$f_1(\omega)^8 - f_2(\omega)^8 = a f^2(\omega).$$

Nimmt man hierzu die Gleichungen:

$$f_1^8 = f_2^8 = f^8, \quad f f_1 f_2 = \sqrt{2},$$

so erhält man

(29) $$f^{24} - a^2 f^{12} - 64 = 0.$$

Durch diese quadratische Gleichung ist f^{12} als Funktion von a bestimmt.

Dann sind die Wurzeln der Gleichung (28) durch die Quadratwurzeln aus den Ausdrücken (22) dargestellt. Das doppelte Vorzeichen dieser Quadratwurzeln erklärt sich daraus, daß zwei entgegengesetzte Werte von a zu derselben Gleichung (29) führen. Man kann aber auch die Wurzeln eindeutig bestimmen nach der Formel (26):

(30) $$z = \frac{a}{w^2 + 5}.$$

In der oben erwähnten Arbeit von Kiepert wird die allgemeine Gleichung fünften Grades auf die Form (15) transformiert, wozu nur die Auflösung einer quadratischen Gleichung erforderlich ist. Sieht man darin a, b, c als beliebig gegeben an, so dienen die Gleichungen (16) zur Bestimmung von λ, μ, γ_3. Dies geschieht ebenfalls mit Hilfe einer quadratischen Gleichung, was allerdings nicht auf den ersten Blick zu ersehen ist. (Vgl. F. Klein, Vorlesungen über das Ikosaëder, S. 191 f.)

Auf die Resolventenbildung für den siebenten Transformationsgrad werden wir weiter unten zurückkommen, wenn wir über die Hilfsmittel verfügen, die uns die komplexe Multiplikation bietet.

ZWEITES BUCH.

QUADRATISCHE KÖRPER.

Neunter Abschnitt.

Diskriminante.

§ 84. Definition der Diskriminanten.

In der Theorie der quadratischen Körper treten als Diskriminanten gewisse ganze rationale (positive oder negative) Zahlen auf, die, wenn sie gerade sind, durch 4 teilbar sind, und wenn sie ungerade sind, bei der Teilung durch 4 den Rest 1 lassen.

Kronecker hat solche Zahlen „Zahlen von Diskriminantenform" genannt. Wir wollen sie hier kurz Diskriminanten nennen, und uns nicht daran stoßen, daß dieses Wort in der Algebra noch mannigfache andere Bedeutungen hat. Wir definieren daher:

1. Eine positive oder negative, von Null verschiedene ganze Zahl, die einer der beiden Kongruenzen

$$D \equiv 0, \qquad D \equiv 1 \pmod 4 \tag{1}$$

genügt, heißt eine Diskriminante.

Jede Quadratzahl ist nach dieser Definition eine Diskriminante. Da diese aber eine gewisse Ausnahmestellung einnehmen, wollen wir sie, wenn die Unterscheidung nötig ist, uneigentliche Diskriminanten nennen.

2. Das Produkt zweier und folglich beliebig vieler Diskriminanten ist wieder eine Diskriminante.

3. Eine Diskriminante, die (außer 1) keinen quadratischen Teiler enthält, nach dessen Absonderung eine Diskriminante übrig bleibt, heißt Stammdiskriminante.

Stammdiskriminanten sollen in der Folge zum Unterschied von anderen mit Δ bezeichnet sein. Ist D keine Stammdiskriminante, so gibt es eine und nur eine Quadratzahl Q^2 und eine Stammdiskriminante Δ, so daß

$$D = \Delta Q^2 \tag{2}$$

ist; Δ heißt dann der Stamm von D.

Eine Stammdiskriminante ist durch keine ungerade Quadratzahl teilbar. Ist aber Δ durch 4 teilbar, so muß

$$(3) \qquad \Delta \equiv 8,\ 12 \pmod{16}$$

sein. Denn wäre $\Delta \equiv 0,4 \pmod{16}$, so würde nach Forthebung des Faktors 4 eine Diskriminante übrig bleiben.

Um also zu einem gegebenen D den Stamm zu finden, hat man zunächst die größte ungerade Quadratzahl und dann noch eine so hohe Potenz von 4 abzusondern, daß Δ entweder ungerade und $\equiv 1 \pmod 4$ oder $\equiv 8$, oder $\equiv 12 \pmod{16}$ wird.

4. Eine eigentliche Diskriminante, die nicht in Faktoren zerlegbar ist, die selbst wieder Diskriminanten sind, heißt Primdiskriminante.

Ist p eine natürliche ungerade Primzahl, und wird das Zeichen $\pm$ so bestimmt, daß $\pm p \equiv 1 \pmod 4$ ist, so gibt es folgende Primdiskriminanten:

$$(4) \qquad \pm p, \quad -4, \quad +8, \quad -8.$$

5. Jede Stammdiskriminante läßt sich auf eine und nur auf eine Weise in Primdiskriminanten zerlegen.

Denn sondert man von Δ zuerst alle Faktoren $\pm p$ ab, so bleibt nur eine der Zahlen $1, -4, +8, -8$ übrig.

§ 85. Das erweiterte Legendre-Jacobische Symbol.

Das Legendresche Symbol $\left(\frac{m}{p}\right)$ hat, wenn m eine beliebige positive oder negative von Null verschiedene Zahl, p eine in m nicht aufgehende natürliche Primzahl ist, den Wert $+1$, wenn m quadratischer Rest, und den Wert -1, wenn m quadratischer Nichtrest von p ist (Bd. I, § 145).

Die Bedeutung des Symbols ist von Jacobi so erweitert worden, daß für p auch eine zusammengesetzte Zahl gesetzt werden kann. Wenn aber m eine Diskriminante ist, so empfiehlt sich bisweilen eine noch weitergehende Verallgemeinerung, die wir jetzt darlegen müssen [1]).

---

[1]) Kronecker, Berliner Sitzungsberichte, 30. Juli 1885. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl., § 186. H. Weber, Göttinger Nachrichten, Januar 1893.

Wenn D eine Diskriminante und n eine ganze rationale Zahl ist, so definieren wir ein Symbol (D, n) durch folgende Bestimmungen:

(1) $$(D, 0) = 0.$$

(2) $$(D, 1) = 1.$$

(3) $$(D, -1) = +1, \quad D > 0.$$
$$= -1, \quad D < 0.$$

(4) $$(D, p) = 0,$$

wenn p ein Primteiler von D ist.

(5) $$(D, 2) = (-1)^{\frac{D^2-1}{8}}, \; D \text{ ungerade.}$$

(6) $$(D, p) = \left(\frac{D}{p}\right),$$

wenn p eine nicht in D aufgehende ungerade Primzahl ist.

Zerlegt man $\pm n$ in seine Primfaktoren

$$n = \pm p, p', p'', \ldots,$$

so ist

(7) $$(D, n) = (D, \pm 1)\,(D, p)\,(D, p')\,(D, p'') \ldots$$

Durch (1) bis (7) ist offenbar das Symbol (D, n) widerspruchslos für alle Zahlen n definiert, und kann nur einen der Werte -1, 0, $+1$ haben. Es ist immer dann und nur dann $= 0$, wenn D und n nicht relativ prim zueinander sind. Aus (7) ergibt sich noch:

(8) $$(D, n)\,(D, n') = (D, n n'),$$

und wenn Q^2 eine Quadratzahl ist, die mit n keinen gemeinsamen Teiler hat,

(9) $$(Q^2 D, n) = (D, n).$$

Die auf das Reziprozitätsgesetz bezüglichen Formeln nehmen in dieser Bezeichnungsweise eine besondere Form an. Wir betrachten zunächst die Primdiskriminanten.

Ist $\pm p \equiv 1 \pmod 4$, so ist nach (3), (5), (6):

$$(\pm p, -1) = (-1)^{\frac{p-1}{4}} = \left(\frac{-1}{p}\right),$$

$$(\pm p, 2) = (-1)^{\frac{p^2-1}{8}} = \left(\frac{2}{p}\right),$$

$$(\pm p, n) = \left(\frac{\pm p}{n}\right) = \left(\frac{n}{p}\right),$$

wenn n eine ungerade Primzahl ist (nach dem Reziprozitätsgesetz und seinen Ergänzungssätzen [Bd. I, § 145, 9.]), und diese Formeln lassen sich zusammenfassen in

$$(10) \qquad (\pm p, n) = \left(\frac{n}{p}\right).$$

Diese Formel gilt aber wegen (7) *für jedes beliebige n, das durch p nicht teilbar ist.*

In gleicher Weise findet man für ein ungerades n:

$$(11) \qquad \begin{aligned} (-4, n) &= (-1)^{\frac{n-1}{2}}, \\ (8, n) &= (-1)^{\frac{n^2-1}{8}}, \\ (-8, n) &= (-1)^{\frac{n-1}{2} + \frac{n^2-1}{8}}. \end{aligned}$$

Weiter ist allgemein, wenn D, D' zwei Diskriminanten sind:

$$(12) \qquad (D, n)\,(D', n) = (DD', n).$$

Diese Formel gilt zunächst, wenn DD' und n nicht relativ prim sind, weil dann beide Seiten $= 0$ sind. Sie gilt ferner für $n = -1$ [nach (3)], für $n = 2$ [nach (5) und der Kongruenz $\frac{D^2-1}{8} + \frac{D'^2-1}{8} \equiv \frac{D^2 D'^2 - 1}{8} \pmod 2$] und für eine ungerade Primzahl n [nach (6)]. Also gilt sie wegen (7) allgemein.

Wir können nun das Reziprozitätsgesetz mit seinen Ergänzungssätzen für Diskriminanten in folgender Weise zusammenfassen:

$$(13) \qquad (D, D') = \pm (D', D),$$

worin das obere Zeichen gilt, wenn von den beiden Diskriminanten D, D' wenigstens eine positiv ist, das untere, wenn beide negativ sind.

Um diese Formel aus der gewöhnlichen Form des Reziprozitätsgesetzes abzuleiten, nehmen wir zunächst an, es gelten die beiden Formeln:

$$\begin{aligned} (D, D') &= \pm (D', D), \\ (D_1, D') &= \pm (D', D_1). \end{aligned}$$

Dann folgt aus (8) und (12)

$$(DD_1, D') = \pm (D', DD_1),$$

worin wieder das untere Zeichen nur dann gilt, wenn D' und DD_1 beide negativ sind. Durch nochmalige Anwendung ergibt sich

$$(DD_1, D'D_1') = \pm (D'D_1', DD_1)$$

und folglich ist die Formel (12) erwiesen, wenn sie für irgend zwei Primdiskriminanten gilt.

Es ist aber nach (10), wenn p und p' ungerade Primzahlen sind:

$$(\pm p, \pm p') = \pm\left(\frac{p'}{p}\right), \quad (\pm p', \pm p) = \pm\left(\frac{p'}{p}\right),$$

worin rechts das negative Zeichen nur dann steht, wenn links beide Zeichen negativ, also p sowohl als $p' \equiv 3 \pmod 4$ sind. In diesem und nur in diesem Falle ist aber $\left(\frac{p'}{p}\right) = -\left(\frac{p}{p'}\right)$, sonst $\left(\frac{p'}{p}\right) = \left(\frac{p}{p'}\right)$. Also ergibt sich für diesen Fall die Formel (13) als richtig.

Ferner ist nach (11) und (3), (5)

$$(-4, \pm p) = +1, \quad (\pm p, -4) = \pm 1,$$

$$(p, \pm 8) = (p, \pm 2) = (p, 2) = (-1)^{\frac{p^2-1}{8}},$$

$$(\pm 8, p) = \left(\frac{\pm 8}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

$$[p \equiv 1 \pmod 4],$$

$$(-p, \pm 8) = (-p, \pm 2) = \pm(-p, 2) = -1,$$

$$(\pm 8, -p) = \pm\left(\frac{\pm 8}{p}\right) = -1,$$

$$[p \equiv 3 \pmod 8],$$

woraus für diese Fälle die Formel (13) folgt, die damit allgemein erwiesen ist.

Aus (13) folgt weiter, da jede Quadratzahl eine positive Diskriminante ist, falls m zu D relativ prim ist,

(14) $$(D, m^2) = 1$$

und folglich nach (8):

(15) $$(D, m^2 n) = (D, n),$$

wenn m und D keinen gemeinschaftlichen Teiler haben.

Wir haben ferner den Satz:

(16) $$(D, n) = (D, n'),$$

wenn $n \equiv n' \pmod D$.

Der Satz ist richtig, wenn n und D einen gemeinschaftlichen Teiler haben, und nach (12) ist er allgemein erwiesen, wenn er für jede Primdiskriminante D gilt. Für diese ergibt er sich aber sofort aus (10), (11).

Nehmen wir an, in (16) seien n, n' selbst Diskriminanten:

$$n = D_1, \quad n' = D_2, \quad D_1 \equiv D_2 \pmod{D},$$

so ist

$$(D, D_1) = (D, D_2)$$

und es folgt aus (13):

$$(D, D_1) = \pm(D_1, D)$$
$$(D, D_2) = \pm(D_2, D),$$

worin die oberen Zeichen gelten, wenn D positiv ist, die unteren, wenn D, D_1, D_2 alle drei negativ sind, und verschiedene Zeichen, wenn D negativ und D_1, D_2 von verschiedenen Vorzeichen sind. Es ist also nach (16):

$$(17) \qquad (D_1, D) = \pm(D_2, D),$$

worin das untere Zeichen nur dann gilt, wenn die beiden Zahlen D und $D_1 D_2$ beide negativ sind.

Sind D_1, D_2 ungerade, so können wir $D = 4m$ setzen, worin m eine beliebige ganze Zahl ist, und wir erhalten aus (17)

$$(18) \qquad (D_1, m) = \pm(D_2, m),$$

wenn

$$(19) \qquad D_1 \equiv D_2 \pmod{4m}$$

ist, und das untere Zeichen nur dann gilt, wenn m und $D_1 D_2$ beide negativ sind.

Dieser Satz ist zunächst bewiesen unter der Voraussetzung, daß D_1 und D_2 ungerade sind. Er gilt aber allgemein. Denn die Kongruenz (19) verlangt zunächst, daß D_1 und D_2 zugleich gerade oder zugleich ungerade seien. Sind sie beide gerade und ist dann m gerade, so ist (18) richtig, weil beide Seiten verschwinden. Ist aber m ungerade, D_1, D_2 gerade, so setze man in (17) $D = \pm m \equiv 1 \pmod{4}$, worin m eine positive ungerade Zahl ist. Dann folgt aus $D_1 \equiv D_2 \pmod{D}$ die Kongruenz (19) und nach (17) ist

$$(20) \qquad \begin{aligned} (D_1, m) &= (D_2, m), \\ (D_1, -m) &= \pm(D_2, -m), \\ (D_1, -1) &= \pm(D_2, -1), \end{aligned}$$

und folglich wieder

$$(D_1, m) = (D_2, m).$$

Also gilt diese Formel für jedes positive ungerade m, und nach (20) ist dann (18) auch für ein negatives m erwiesen. Die Formeln (16) und (18) können zur Berechnung des Symbols (D, n)

nach dem Algorithmus des größten gemeinschaftlichen Teilers dienen. Denn man kann aus den Kongruenzen

$$\begin{aligned} D &\equiv D' \pmod{4n}, \\ n &\equiv n' \pmod{D'}, \\ D' &\equiv D'' \pmod{4n'}, \\ n' &\equiv n'' \pmod{D''}, \\ &\ldots\ldots\ldots \end{aligned}$$

die Reihe der Zahlen

$$D', \quad 2n', \quad D'', \quad 2n'', \ldots$$

so bestimmen, daß jede folgende dem absoluten Werte nach kleiner ist als die vorhergehende, solange keine der Zahlen $n', n'', n''', \ldots$ gleich ± 1 geworden ist.

Ist D keine Quadratzahl, so läßt sich immer eine Zahl β so bestimmen, daß

(21) $$(D, \beta) = -1.$$

Ist nämlich Δ der Stamm von D und ist β relativ prim zu D, so ist (nach 9)

$$(D, \beta) = (\Delta, \beta).$$

Ist $\Delta = \delta \Delta'$ und δ eine Primdiskriminante, also relativ prim zu Δ', so kann man β_0 so annehmen, daß

$$(\delta, \beta_0) = -1$$

wird [nach (10) und (11)] und man kann β aus den beiden Kongruenzen

$$\begin{aligned} \beta &\equiv \beta_0 \pmod{\delta}, \\ &\equiv 1 \pmod{\Delta'} \end{aligned}$$

bestimmen. Dann erhält man nach (12)

$$(D, \beta) = (\delta, \beta_0) = -1.$$

Läßt man s ein volles Restsystem nach dem Modul D durchlaufen und setzt

$$S = \sum^{s} (D, s),$$

so folgt durch Multiplikation mit (D, β)

$$-S = \sum^{s} (D, \beta s),$$

und da βs zugleich mit s ein Restsystem durchläuft, so folgt

(22) $$S = 0.$$

Es folgt hieraus:

In einem vollständigen System inkongruenter, zu D teilerfremder Zahlen s gibt es ebensoviele Zahlen α, für die $(D, \alpha) = +1$ ist, wie Zahlen β, für die $(D, \beta) = -1$ ist, und es ist

$$\begin{aligned}(D, n) &= +1, \quad \text{wenn } n \equiv \alpha \\ &= -1, \quad \quad " \quad n \equiv \beta\end{aligned} \pmod{D}.$$

§ 86. Die Gaussschen Summen.

Wir haben im ersten Bande die Gaussschen Summen aus der Theorie der Kreisteilung kennen gelernt. Diese Ausdrücke lassen sich verallgemeinern und nehmen durch Anwendung des Symbols (D, n) eine einfache Gestalt an.

Es war [Bd. I, § 179, (16)], wenn n eine ungerade Primzahl, s eine durch n nicht teilbare Zahl bedeutet und k ein Restsystem nach dem Modul n durchläuft:

$$(1) \qquad \sum \left(\frac{k}{n}\right) e^{\frac{2\pi i s k}{n}} = \left(\frac{s}{n}\right) i^{\left(\frac{n-1}{2}\right)^2} \sqrt{n}.$$

Setzen wir $\pm n = \Delta \equiv 1 \pmod{4}$, so ist Δ eine Primdiskriminante, und es ist nach § 85, (10)

$$\left(\frac{k}{n}\right) = (\Delta, k), \left(\frac{\mp s}{n}\right) = (\Delta, \mp s) = (\Delta, s)$$

[letzteres nach § 85, (3), da die oberen Zeichen bei positiven, die unteren bei negativen Δ gelten], ferner:

$$i^{\left(\frac{n-1}{2}\right)^2} \sqrt{n} = \sqrt{\Delta},$$

wenn $\sqrt{\Delta}$ positiv reell oder positiv imaginär ist, je nachdem $n \equiv 1$ oder $\equiv 3 \pmod{4}$ ist, und wir können (1) in der Form schreiben:

$$(2) \qquad \sum^{k} (\Delta, k)\, e^{-\frac{2\pi i k s}{\Delta}} = (\Delta, s) \sqrt{\Delta},$$

wenn wir im Falle, wo Δ positiv ist, s durch $-s$ ersetzen. Diese Formel ist zunächst nur für eine ungerade Primdiskriminante erwiesen. Sie gilt aber auch, wie die direkte Rechnung zeigt, für

$$\Delta = -4, \quad 8, \quad -8,$$

also für jede Primdiskriminante.

Setzen wir die Richtigkeit der Formel (2) für $\Delta = \Delta'$, $\Delta = \Delta''$ voraus, so folgt, wenn Δ' und Δ'' keinen gemeinschaftlichen Teiler haben, ihre Richtigkeit für $\Delta = \Delta' \Delta''$.

Es ist nämlich

$$(3) \qquad \sqrt{\Delta'}\,\sqrt{\Delta''} = \pm \sqrt{\Delta' \Delta''},$$

wenn das obere Zeichen gilt, falls von den beiden Stammdiskriminanten $\varDelta'$, $\varDelta''$ wenigstens eine positiv ist, das untere, wenn beide negativ sind.

Setzen wir

$$k = k'\varDelta'' + k''\varDelta',$$

und lassen k', k'' Restsysteme nach $\varDelta'$, $\varDelta''$ durchlaufen, so durchläuft k ein Restsystem nach $\varDelta = \varDelta'\varDelta''$.

Die Multiplikation der beiden Summen

$$(4) \qquad \sum^{k'} (\varDelta', k')\, e^{-\frac{2s\pi i k'}{\varDelta'}}, \quad \sum^{k''} (\varDelta'', k'')\, e^{-\frac{2s\pi i k''}{\varDelta''}}$$

ergibt

$$(5) \qquad \sum^{k'k''} (\varDelta', k')\,(\varDelta'', k'')\, e^{-\frac{2s\pi i k}{\varDelta}}.$$

Es ist aber nach § 85, (16)

$$(\varDelta', k) = (\varDelta', \varDelta'')\,(\varDelta', k'),$$
$$(\varDelta'', k) = (\varDelta'', \varDelta')\,(\varDelta'', k''),$$

und folglich nach § 85, (13)

$$(\varDelta, k) = \pm(\varDelta', k')\,(\varDelta'', k''),$$

und demnach ergibt sich aus (3), (4) und (5) die allgemeine Gültigkeit der Formel (2) für jede Stammdiskriminante $\varDelta$.

Zehnter Abschnitt.

Algebraische Zahlen und Formen.

§ 87. Ideale und Formen in algebraischen Körpern.

Das Interesse, das die Theorie der elliptischen Funktionen für den Algebraiker hat, entspringt aus ihrer Anwendung auf die Theorie der quadratischen Irrationalzahlen, zu denen sie in einer analogen Beziehung stehen, wie die Einheitswurzeln zu den rationalen Zahlen. Sie bieten uns das erste und bisher einzige in seinen Gesetzen genauer bekannte Beispiel eines Gebietes algebraischer Zahlen, die über die Kreisteilungszahlen hinausgehen. Um die Theorie dieser Zahlen eingehender darstellen zu können, müssen wir einige Sätze aus der Theorie der Formen und algebraischen Körper und speziell der quadratischen Formen vorausschicken.

In Bd. II, § 163, 169 hat sich ein Zusammenhang ergeben zwischen den Idealen eines algebraischen Körpers Ω vom $n$ten Grade und gewissen homogenen Funktionen $n$ten Grades von n Variablen. Ehe wir dies auf quadratische Körper anwenden, sei kurz an die allgemeinen Sätze erinnert.

Es sei $\mathfrak{a}$ ein Ideal eines Körpers Ω und $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis dieses Ideals. Ferner sei $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis von Ω. Dann ist

(1) $$(\alpha_1, \alpha_2, \ldots, \alpha_n) = (A)\,(\omega_1, \omega_2, \ldots, \omega_n),$$

wenn (A) eine lineare Substitution mit ganzzahligen Koeffizienten bedeutet. Um zu einer anderen Basis $\alpha'_1, \alpha'_2, \ldots, \alpha'_n$ von $\mathfrak{a}$ überzugehen, mache man eine lineare Substitution L mit der Determinante ± 1,

(2) $$(\alpha'_1, \alpha'_2, \ldots, \alpha'_n) = (L)\,(\alpha_1, \alpha_2, \ldots, \alpha_n),$$

woraus sich ergibt

(3) $$(\alpha'_1, \alpha'_2, \ldots, \alpha'_n) = (L)\,(A)\,(\omega_1, \omega, \ldots, \omega_n)$$ [1].

[1]) Über lineare Substitutionen und ihre Zusammensetzung vergleiche man den sechsten Abschnitt des zweiten Bandes.

Unter der Norm $N(\mathfrak{a})$ des Ideals $\mathfrak{a}$ versteht man den absoluten Wert der Determinante A der Substitution (A):

$$A = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{n,n},$$

und nach (3) ist die Norm unabhängig von der Wahl der Basis.

1. Wir wollen die Basis (α_ν) positiv nennen, wenn die Determinante A positiv, also der Norm von $\mathfrak{a}$ gleich ist. Ist (α_ν) positiv, so ist (α'_ν) immer dann positiv, wenn die Substitutionsdeterminante $L = +1$ ist.

Man kann aus jeder Basis durch eine Substitution mit der Determinante -1, also z. B. durch Vertauschung zweier α_ν, eine positive Basis ableiten, und wir werden in der Folge meist nur positive Basen verwenden.

Die in Bd. II, § 163, (3) bestimmte Basis ist positiv.

Bedeutet nun $t_1, t_2, \ldots, t_n$ ein System unabhängiger Variablen und

(4) $$\lambda = \sum^{\nu} \alpha_\nu t_\nu$$

eine Basisform mit positiver Basis, so ergibt sich (Bd. II, § 164)

(5) $$N(\lambda) = N(\mathfrak{a})\, T,$$

worin

(6) $$T = \Sigma \pm t_{1,1}\, t_{2,2} \ldots t_{n,n}$$

eine primitive ganzzahlige homogene Form $n$ten Grades der Variablen t_ν ist. Die $t_{r,s}$ sind lineare Funktionen der t_ν.

Wendet man auf (4) die Substitution (2) an, so ergibt sich

(7) $$\lambda = \lambda' = \Sigma\, \alpha'_\nu t'_\nu,$$

wenn

(8) $$(t_1, t_2, \ldots, t_n) = L'(t'_1, t'_2, \ldots, t'_n),$$

worin L' die transponierte Substitution von L ist, und wenn (α'_ν) gleichfalls eine positive Basis ist, so hat L' die Determinante $+1$ und die Formel (5) ergibt

(9) $$N(\lambda) = N(\mathfrak{a})\, T',$$

worin T' eine homogene Funktion $n$ten Grades der Variablen t' ist, die durch die Substitution (8) aus T hervorgeht.

Zwei Formen, die durch ganzzahlige lineare Substitution mit der Determinante $+1$ auseinander hervorgehen, heißen äquivalent. Bisweilen werden die Formen auch dann äquivalent genannt, wenn die Substitutionsdeterminante -1 ist, dann aber mit dem Zusatze „uneigentlich". Es ist dann durch (8) bewiesen:

2. Nennen wir die Form T die zu der Basis (α_ν) von $\mathfrak{a}$ gehörige Form, so sind die zu verschiedenen positiven Basen desselben Ideals gehörigen Formen äquivalent.

Bezeichnen wir die konjugierten Werte von α_s, ω_s mit

$$\alpha_{s,1},\ \alpha_{s,2},\ \ldots,\ \alpha_{s,n};\quad \omega_{s,1},\ \omega_{s,2},\ \ldots,\ \omega_{s,n}$$

und setzen

$$\alpha_{s,r} = \sum^{\nu} a_{s,\nu}\,\omega_{\nu,r}, \tag{10}$$

so ergibt sich

$$(\Sigma \pm \alpha_{1,1}\,\alpha_{2,2}\ldots\alpha_{n,n})^2 = N(\mathfrak{a})^2 \varDelta, \tag{11}$$

wenn $\varDelta$ die Grundzahl des Körpers Ω, nämlich das Determinantenquadrat:

$$\varDelta = (\Sigma \pm \omega_{1,1}\,\omega_{2,2}\ldots\omega_{n,n})^2$$

ist (Bd. II, § 162).

Sind $\lambda_1, \lambda_2, \ldots, \lambda_n$ die konjugierten Werte von λ, so ist nach (4)

$$\lambda_r = \sum^{\nu} \alpha_{\nu,r}\,t_\nu \tag{12}$$

eine lineare Substitution für die Variablen t_ν mit der Substitutionsdeterminante

$$r = N(\mathfrak{a})\sqrt{\varDelta}, \tag{13}$$

und durch diese geht nach (5) die Form T in das Produkt

$$T' = [N(\mathfrak{a})]^{-1}\lambda_1\,\lambda_2\ldots\lambda_n \tag{14}$$

über, weil $N(\lambda)$ das Produkt der konjugierten Werte von λ ist (Bd. II, § 151). Wir können hierauf die Invariantentheorie (Bd. I, § 65) anwenden, und wenn wir die Hessesche Determinante bilden:

$$H = \Sigma \pm \frac{\partial^2 T}{\partial t_1\,\partial t_1}\,\frac{\partial^2 T}{\partial t_2\,\partial t_2}\cdots\frac{\partial^2 T}{\partial t_n\,\partial t_n}, \tag{15}$$

so ist

$$H' = r^{-2} H. \tag{16}$$

Wenn wir aber H' nach (14) in den Variablen λ_ν bilden, und beachten, daß eine n-reihige Determinante, in der die Diagonalglieder $= 0$ und alle anderen Glieder $= 1$ sind, den Wert $(-1)^{n-1}(n-1)$ hat[1]), so folgt:

[1]) Man kann diesen Satz leicht beweisen, wenn man die Determinante durch Zufügung einer $(n+1)$ten Zeile und einer $(n+1)$ten Spalte erweitert, bei der in der hinzugefügten Zeile nur Einer, in der Spalte mit Ausnahme des letzten Elementes Nullen stehen.

$$H' = (-1)^{n-1}(n-1)\,N(\mathfrak{a})^{-n}(\lambda_1\lambda_2\ldots\lambda_n)^{n-2},$$
$$= (-1)^{n-1}(n-1)\,N(\mathfrak{a})^{-2}\,T^{n-2}$$

und folglich nach (13) und (16)

(17) $$H = (-1)^{n-1}(n-1)\,T^{n-2}\Delta.$$

§ 88. Idealklassen und Formenklassen.

Wir haben in Bd. II, § 170 die Äquivalenz der Ideale und die Idealklassen erklärt. Danach waren zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ äquivalent, wenn es eine ganze oder gebrochene Zahl des Körpers Ω gibt, die der Quotient von $\mathfrak{b}$ und $\mathfrak{a}$ ist, also:

(1) $$\eta\,\mathfrak{a} = \mathfrak{b},$$

und es hat sich gezeigt, daß danach die Ideale in Klassen eingeteilt werden, und daß die Zahl dieser Klassen endlich ist. In manchen Fällen ist es zweckmäßig, den Äquivalenzbegriff etwas enger zu fassen und $\mathfrak{a}$ und $\mathfrak{b}$ nur dann äquivalent zu nennen, wenn es eine der Bedingung (1) genügende Zahl η mit positiver Norm gibt. Dieser Unterschied kommt natürlich nicht in Betracht, wenn die Normen aller Zahlen positiv sind, wie z. B. im imaginären quadratischen Körper. Auch dann kommt er nicht in Betracht, wenn es Einheiten mit der Norm -1 gibt, weil, wenn ε eine solche Einheit ist, entweder $N(\eta)$ oder $N(\varepsilon\eta)$ positiv ist und ε und $\varepsilon\eta$ gleichzeitig der Bedingung (1) genügen.

Gibt es aber keine Einheiten, deren Norm $= -1$ ist, wohl aber andere Zahlen in Ω mit negativer Norm, so teilt sich bei der engeren Definition der Äquivalenz jede Idealklasse noch einmal in zwei Klassen. Wir wollen hier den engeren Äquivalenzbegriff festhalten, der z. B. bei manchen reellen quadratischen Körpern in Kraft tritt[1]).

In (1) kann η gebrochen sein. Ist aber α eine durch $\mathfrak{a}$ teilbare ganze Zahl, so ist $\eta\alpha$ eine durch $\mathfrak{b}$ teilbare ganze Zahl, und daraus ergibt sich: Wenn

(2) $$(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

eine Basis von $\mathfrak{a}$ ist, so ist

$$(\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1\eta, \alpha_2\eta, \ldots, \alpha_n\eta)$$

eine Basis von $\mathfrak{b}$, und wenn die erste Basis positiv ist, so ist es (bei dem engeren Äquivalenzbegriff) auch die zweite.

[1]) Wenn nämlich die Pellsche Gleichung $t^2 - Du^2 = -4$ keine Lösung hat.

Denn die notwendige und hinreichende Bedingung, daß (2) Basis von $\mathfrak{a}$ sei, besteht darin, daß jede durch $\mathfrak{a}$ teilbare ganze Zahl α und nur solche in der Form:

(3) $$\alpha = x_1 \alpha_1 + x_2 \alpha_2 + \cdots + x_n \alpha_n$$

mit ganzzahligen $x_1, x_2, \ldots, x_n$ enthalten ist. Folglich sind alle Zahlen

(4) $$\beta = x_1 \alpha_1 \eta + x_2 \alpha_2 \eta + \cdots + x_n \alpha_n \eta$$

durch $\mathfrak{b}$ teilbar. Ist umgekehrt β eine durch $\mathfrak{b}$ teilbare ganze Zahl, so ist β/η durch $\mathfrak{a}$ teilbar und folglich in der Form (3) darstellbar. Mithin ist β durch (4) darstellbar.

Ferner ist nach der Bezeichnung von (9) und (10), § 87, wenn α eine positive Basis ist:

$$\begin{aligned} \Sigma \pm \alpha_{1,1}\, \alpha_{2,2} \ldots \alpha_{n,n} &= N(\mathfrak{a})\, \Sigma \pm \omega_{1,1}\, \omega_{2,2} \ldots \omega_{n,n}, \\ \Sigma \pm \beta_{1,1}\, \beta_{2,2} \ldots \beta_{n,n} &= N(\eta)\, \Sigma \pm \alpha_{1,1}\, \alpha_{2,2} \ldots \alpha_{n,n}, \\ &= N(\eta)\, N(\mathfrak{a})\, \Sigma \pm \omega_{1,1}\, \omega_{2,2} \ldots \omega_{n,n}, \\ &= \pm N(\mathfrak{b})\, \Sigma \pm \omega_{1,1}\, \omega_{2,2} \ldots \omega_{n,n}, \end{aligned}$$

und da nach (1)

(5) $$N(\mathfrak{b}) = N(\eta)\, N(\mathfrak{a})$$

ist, so muß bei $\pm N(\mathfrak{b})$ das positive Zeichen stehen.

Ist λ eine Basisform von $\mathfrak{a}$, so ist $\eta\lambda$ eine Basisform von $\mathfrak{b}$, und

(6) $$\begin{aligned} N(\lambda) &= N(\mathfrak{a})\, T, \\ N(\eta\lambda) &= N(\mathfrak{b})\, T, \end{aligned}$$

und zu den beiden Idealen $\mathfrak{a}$, $\mathfrak{b}$ gehört also dieselbe Form T. Vereinigen wir äquivalente Formen T in eine Klasse, so können wir nach 2. sagen:

3. Zu jeder Idealklasse gehört eine bestimmte Formenklasse.

Bei der Beantwortung der Frage, ob zu einer und derselben Formenklasse verschiedene Idealklassen gehören können, machen wir die Voraussetzung, daß Ω ein Normalkörper sei: Nehmen wir also an, zu zwei Idealen $\mathfrak{a}$ und $\mathfrak{a}'$ gehören äquivalente Formen T und T', so ist, wenn λ eine Basisform von $\mathfrak{a}$ ist,

(7) $$N(\lambda) = N(\mathfrak{a})\, T,$$

und wenn wir T' durch eine lineare Substitution in T überführen, und unter λ' eine Basisform von $\mathfrak{a}'$ (mit denselben Variablen t wie λ) verstehen, so ist

(8) $$N(\lambda') = N(\mathfrak{a}')\, T.$$

Die linearen Faktoren von $N(\lambda)$ und $N(\lambda')$ müssen also, von einem konstanten Faktor abgesehen, miteinander übereinstimmen, weil man eine ganze Funktion beliebiger Variablen nur auf eine Weise in irreducible (hier lineare) Faktoren zerlegen kann (Bd. I, § 20, Bd. II, § 152), und da alle diese Faktoren demselben Körper Ω angehören, so gibt es unter den konjugierten Faktoren λ' einen, der der Bedingung genügt:

$$\lambda = \eta\,\lambda',$$

worin η eine Zahl in Ω ist. Die Funktionale λ und λ' und demnach die entsprechenden Ideale sind also äquivalent.

4. Gehört in einem Normalkörper zu den zwei Idealen $\mathfrak{a}$ und $\mathfrak{a}'$ dieselbe Formenklasse, so gibt es unter den mit $\mathfrak{a}'$ konjugierten Idealen eines, das mit $\mathfrak{a}$ äquivalent ist.

§ 89. Komposition der Formen und Multiplikation der Ideale.

Es seien jetzt $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale in Ω und

$$\mathfrak{c} = \mathfrak{a}\,\mathfrak{b} \tag{1}$$

das aus beiden gebildete Produkt. Es seien ferner

$$\begin{aligned} \mathfrak{a} &= (\alpha_1, \alpha_2, \ldots, \alpha_n), \\ \mathfrak{b} &= (\beta_1, \beta_2, \ldots, \beta_n), \\ \mathfrak{c} &= (\gamma_1, \gamma_2, \ldots, \gamma_n), \end{aligned} \tag{2}$$

Basen dieser Ideale. Da jede Zahl $\alpha_h\beta_k$ zu $\mathfrak{c}$ gehört, so gibt es ein System ganzer rationaler Zahlen $c_{h\,k}^{(r)}$, so daß

$$\alpha_h\,\beta_k = \sum^{r} c_{h,k}^{(r)}\,\gamma_r \tag{3}$$

wird, und da jede Zahl in $\mathfrak{c}$ durch Multiplikation je einer Zahl aus $\mathfrak{a}$ und aus $\mathfrak{b}$ und Addition dieser Produkte entsteht (Bd. II, § 169), so ist auch umgekehrt

$$\gamma_s = \sum^{h,k} a_{h,k}^{(s)}\,\alpha_h\,\beta_k, \tag{4}$$

worin die $a_{h,k}^{(s)}$ gleichfalls ganze rationale Zahlen sind.

Setzt man (3) in (4) ein, so folgt

$$\gamma_s = \sum^{r} \gamma_r \sum^{h,k} a_{h,k}^{(s)}\,c_{h,k}^{(r)}, \tag{5}$$

und daraus

$$\sum^{h,k} a_{h,k}^{(s)}\,c_{h,k}^{(r)} = (r, s), \tag{6}$$

worin

$$(r, r) = 1, \quad (r, s) = 0, \quad r \neq s.$$

Bezeichnen wir also mit x_r Variable und setzen

(7) $$\sum^{r} x_r\, c_{h,k}^{(r)} = y_{h,k},$$

so folgt:

(8) $$x_s = \sum^{h,k} a_{h,k}^{(s)}\, y_{h,k}.$$

Jetzt bedeuten u_r, v_r, t_r drei Systeme von Variablen und

(9) $$\mu = \Sigma\, \alpha_r u_r,\quad \nu = \Sigma\, \beta_r v_r,\quad \lambda = \Sigma\, \gamma_r t_r$$

Basisformen von $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ferner U, V, T die zu $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ gehörigen Formen, in den Variablen u, v, t geschrieben. Es ist dann

(10) $$N(\mu) = N(\mathfrak{a})\,U,\quad N(\nu) = N(\mathfrak{b})\,V,\quad N(\lambda) = N(\mathfrak{c})\,T.$$

Es ergibt sich also aus (3) durch Multiplikation mit $u_h v_k$ und Summation nach (9):

(11) $$\mu\nu = \sum^{r} \gamma_r \sum^{h,k} c_{h,k}^{(r)} u_h v_k,$$

also, wenn man

(12) $$t_r = \sum^{h,k} c_{h,k}^{(r)} u_h v_k$$

setzt:

(13) $$\mu\nu = \lambda,$$

und daraus, da $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{c})$, ist nach (10)

(14) $$T = UV.$$

Darin sind aber die t_r nicht mehr unabhängige Variable, sondern sie gehen durch die bilineare Substitution (12) aus u_h, v_k hervor.

5. Die Form T geht durch die bilineare Substitution (12) in das Produkt der beiden Formen U, V über.

Diese Substitution hat aber noch eine wesentliche Eigentümlichkeit. Wir nennen die durch (12) bestimmten Funktionen t_r nach einem Primzahlmodul p linear unabhängig, wenn aus der Kongruenz

(15) $$\Sigma\, x_r t_r \equiv 0 \pmod{p},$$

in dem die x_r ganze rationale Zahlen sind, folgt, daß diese Zahlen alle durch p teilbar sind. Findet dies für jede beliebige Primzahl p statt, so heißen die t_r schlechthin linear unabhängig.

Die Kongruenz (15) ist nach (12) und (7) gleichbedeutend mit den n^2-Kongruenzen

$$y_{h,k} = \sum^{r} x_r c_{h,k}^{(r)} \equiv 0 \pmod{p}$$

und aus (6) folgt alsdann:

$$x_s \equiv 0 \pmod{p},$$

und dies besagt, daß die Substitutionen (17) für jeden Modul p linear unabhängig sind.

Nach Gauss (Disq. aritm. art. 235) heißt eine Form T aus den beiden Formen U, V komponiert oder zusammengesetzt, wenn T durch eine bilineare Substitution für die Variable t, deren Gleichungen für jeden Modul linear unabhängig sind, in das Produkt $U V$ übergeht.

Danach haben wir den Satz:

6. Die Form, die zu dem Produkt zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$ gehört, ist aus den Formen der Ideale $\mathfrak{a}$ und $\mathfrak{b}$ komponiert[1]).

[1]) Die Sätze, die Gauss an der erwähnten Stelle durch sehr weitläufige Rechnung für binäre quadratische Formen beweist, sind hier in größter Allgemeinheit durch einfache Betrachtungen abgeleitet. Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, § 182. Für binäre quadratische Formen: Dedekind, Crelles Journal, Bd. 129; H. Weber, Göttinger Nachrichten 1907.

Elfter Abschnitt.

Ideale in quadratischen Körpern.

---

§ 90. Diskriminante des quadratischen Körpers.

Ein quadratischer Körper entsteht, wenn man dem Körper der rationalen Zahlen eine Quadratwurzel $\sqrt{d}$ adjungiert, hier kann d als ganze Zahl ohne quadratischen Teiler angenommen werden. Der Körper ist reell oder imaginär, je nachdem d positiv oder negativ ist. Bezeichnet man den Körper der rationalen Zahlen, den absoluten Rationalitätsbereich, mit $\mathfrak{R}$ und mit $\mathfrak{R}(x, x', \ldots)$ den Körper, der durch Adjunktion von $x, x', \ldots$ zu $\mathfrak{R}$ entsteht, so ist der quadratische Körper Ω so zu bezeichnen:

(1) $$\Omega = \mathfrak{R}(\sqrt{d}).$$

Jede Zahl des Körpers Ω kann in die Form gesetzt werden:

(2) $$\omega = \frac{x + y\sqrt{d}}{2},$$

worin x, y rationale ganze oder gebrochene Zahlen sind.

Die zu ω konjugierte Zahl

(3) $$\omega' = \frac{x - y\sqrt{d}}{2}$$

ist gleichfalls in dem Körper Ω enthalten, und folglich ist Ω ein Normalkörper.

Damit ω eine ganze Zahl sei, ist notwendig, daß

$$\omega + \omega' = x, \quad (\omega - \omega')^2 = y^2 d$$

ganze rationale Zahlen sind, und da d keinen quadratischen Teiler haben soll, so müssen x und y ganze Zahlen sein. Damit aber auch ω wirklich eine ganze Zahl sei, muß auch noch die Norm $\frac{1}{4}(x^2 - y^2 d)$ eine ganze rationale Zahl sein, d. h. es muß

(4) $$x^2 - y^2 d \equiv 0 \pmod 4$$

sein. Ist $d \equiv 2$ oder $\equiv 3 \pmod 4$, so kann diese Bedingung nur erfüllt sein, wenn x und y gerade Zahlen sind, und wenn wir also x, y durch $2x, 2y$ ersetzen, folgt:

1. Ist $d \equiv 2, 3 \pmod 4$, so sind alle und nur die Zahlen des Körpers Ω ganz, die in der Form

$$x + y\sqrt{d}$$

mit ganzem rationalen x, y enthalten sind.

Ist aber $d \equiv 1 \pmod 4$, so ist (3) befriedigt, wenn x und y beide gerade oder beide ungerade sind, also wenn x die Form $2x_1 - y$ hat. Ersetzt man dann wieder x_1 durch x, so folgt:

2. Ist $d \equiv 1 \pmod 4$, so sind alle und nur die Zahlen in Ω ganz, die in der Form

$$x + y\,\frac{-1 + \sqrt{d}}{2}$$

mit ganzen rationalen x, y enthalten sind.

Es ist also im Falle 1. $(1, \sqrt{d})$, im Falle 2. $\left(1, \frac{-1+\sqrt{d}}{2}\right)$ eine Minimalbasis des Körpers Ω. Die Grundzahl oder Diskriminante des Körpers Ω ist also im Falle 1.:

$$\Delta = \begin{vmatrix} 1, & \sqrt{d} \\ 1, & -\sqrt{d} \end{vmatrix}^2 = 4d, \tag{5}$$

im Falle 2.:

$$\Delta = \begin{vmatrix} 1, & \frac{-1+\sqrt{d}}{2} \\ 1, & \frac{-1-\sqrt{d}}{2} \end{vmatrix}^2 = d. \tag{6}$$

In beiden Fällen kann man also die ganze Zahl ω in die Form setzen:

$$\omega = \frac{x + y\sqrt{\Delta}}{2}, \tag{7}$$

mit der Bedingung, daß

$$4N(\omega) = x^2 - \Delta y^2 \equiv 0 \pmod 4 \tag{8}$$

sei.

Die beiden Formen der Minimalbasis, die wir erhalten haben, nämlich $(1, \sqrt{d})$ und $\left(1, \frac{-1+\sqrt{d}}{2}\right)$, sind also:

$$\begin{aligned} (1, \theta) &= (1, \tfrac{1}{2}\sqrt{\Delta}), & \Delta &\equiv 0, \\ &= \left(1, \frac{-1+\sqrt{\Delta}}{2}\right), & \Delta &\equiv 1. \end{aligned} \pmod 4. \tag{9}$$

Hierin kann das Vorzeichen von $\sqrt{\Delta}$ in beliebiger Weise bestimmt werden, soll aber dann in derselben Betrachtung festgehalten werden. Wir wollen ein für allemal annehmen:

3. Wenn Δ positiv ist, soll $\sqrt{\Delta}$ gleichfalls positiv sein, und wenn Δ negativ ist, soll $-i\sqrt{\Delta}$ positiv, oder $\sqrt{\Delta}$ positiv imaginär sein.

Aus (1), (2) ergibt sich noch:

4. Die Grundzahl eines quadratischen Körpers ist immer $\equiv 0$ oder $\equiv 1$ nach dem Modul 4 und hat, außer 4, keinen quadratischen Teiler. Sie ist also Diskriminante und zwar Stammdiskriminante.

§ 91. Ideale und Formen in quadratischen Körpern.

Ist $\mathfrak{a}$ ein Ideal des quadratischen Körpers Ω, α_1, α_2 eine positive Basis, und

(1) $$\lambda = \alpha_1 t_1 + \alpha_2 t_2$$

eine Basisform von $\mathfrak{a}$, so ist

(2) $$N(\lambda) = (\alpha_1 t_1 + \alpha_2 t_2)(\alpha_1' t_1 + \alpha_2' t_2) = N(\mathfrak{a})\, T,$$

und $N(\mathfrak{a})$ ist der größte gemeinschaftliche Teiler der drei ganzen rationalen Zahlen

$$\alpha_1 \alpha_1', \quad \alpha_1 \alpha_2' + \alpha_2 \alpha_1', \quad \alpha_2 \alpha_2'.$$

Setzen wir also

(3) $$\begin{aligned} \alpha_1 \alpha_1' &= a\, N(\mathfrak{a}), \\ \alpha_1 \alpha_2' + \alpha_2 \alpha_1' &= b\, N(\mathfrak{a}), \\ \alpha_2 \alpha_2' &= c\, N(\mathfrak{a}), \end{aligned}$$

so ist

(4) $$T = a t_1^2 + b t_1 t_2 + c t_2^2$$

die zur Basis α_1, α_2 gehörige Form. Wir bezeichnen sie, wenn es auf die Bezeichnung der Variablen nicht ankommt, mit

(5) $$\varphi = (a, b, c).$$

Es ist eine primitive quadratische Form, deren Diskriminante

(6) $$\Delta = b^2 - 4ac$$

gleich der Grundzahl des Körpers Ω ist (§ 87). Um die Basis α_1, α_2 nach Bd. II, § 163 zu bilden, suche man zunächst die kleinste durch $\mathfrak{a}$ teilbare natürliche Zahl a_{11} und hierauf die kleinste natürliche Zahl a_{22}, für die sich eine rationale, der Bedingung

(7) $$a_{12} + a_{22}\,\theta \equiv 0 \pmod{\mathfrak{a}}$$

genügende Zahl a_{12} bestimmen läßt. Da die Kongruenz (7) für $a_{22} = a_{11}$ befriedigt werden kann, nämlich durch $a_{12} = 0$, so

folgt, daß a_{11} durch a_{22} teilbar ist, und wir setzen $a_{11} = a_{22}\,a$. Dann haben wir die Basis von $\mathfrak{a}$:

$$
\begin{aligned}
\alpha_1 &= a_{22}\,a, \\
\alpha_2 &= a_{12} + a_{22}\,\theta.
\end{aligned} \tag{8}
$$

Es ist dann nach Bd. II, § 164, (12):

$$N(\mathfrak{a}) = a_{22}^2\,a, \tag{9}$$

und wenn wir für $(1, \theta)$ die Basis § 90, (9) nehmen, so ist

$$
\begin{aligned}
\theta + \theta' &= 0 \text{ oder } = -1, \\
\theta\theta' &= -\tfrac{1}{4}\Delta \text{ oder } = \frac{1-\Delta}{4}.
\end{aligned} \tag{10}
$$

Je nachdem $\Delta \equiv 0$, oder $\equiv 1 \pmod 4$ ist, und

$$(\theta - \theta')^2 = \Delta.$$

Es wird dann in diesen beiden Fällen, wenn man (8) in (3) substituiert und (9) berücksichtigt:

$$a_{22}\,b = 2\,a_{12} \text{ oder } = 2\,a_{12} - a_{22},$$

und folglich in beiden Fällen:

$$\alpha_1 = a_{22}\,a, \quad \alpha_2 = a_{22}\,\frac{b + \sqrt{\Delta}}{2}, \tag{11}$$

und die Form

$$T = (a, b, c)$$

hat hier einen positiven ersten Koeffizienten.

Setzen wir

$$\omega = -\frac{\alpha_2}{\alpha_1} = -\frac{b + \sqrt{\Delta}}{2\,a}, \tag{12}$$

so ist ω Wurzel der quadratischen Gleichung:

$$a\,\omega^2 + b\,\omega + c = 0 \tag{13}$$

und

$$\lambda = a_{22}\,a\,(x - \omega\,y) \tag{14}$$

ist ein dem Ideal $\mathfrak{a}$ entsprechendes Funktional und zugleich eine Basisform von $\mathfrak{a}$. a ist die kleinste positive ganze Zahl, für die $a\,\omega$ eine ganze Zahl wird.

Die notwendige und hinreichende Bedingung dafür, daß zwei ganze Zahlen α_1, α_2 des Körpers Ω die Basis eines Ideals bilden, besteht darin, daß zunächst α_1, α_2 eine Basis des Körpers Ω ist, und daß, wenn ω_1, ω_2 eine Minimalbasis dieses Körpers ist,

$$\alpha_1\,\omega_1, \quad \alpha_2\,\omega_1, \quad \alpha_1\,\omega_2, \quad \alpha_2\,\omega_2$$

durch die Linearform

$$\lambda = \alpha_1\,t_1 + \alpha_2\,t_2$$

mit ganzzahligen t_1, t_2 darstellbar sind (Bd. II, § 163, 164). Denn dann ist, wenn α durch λ darstellbar ist, auch jedes Produkt $\omega\alpha$ durch λ darstellbar. Für unseren Fall reduziert sich diese Bedingung darauf, daß $\alpha_1\theta$, $\alpha_2\theta$ durch λ darstellbar sein müssen. Ist aber (a, b, c) irgend eine quadratische Form der Diskriminanten Δ mit positivem ersten Koeffizienten a, so können wir für θ auch $\frac{1}{2}(b + \sqrt{\Delta})$ nehmen und da

$$\left(\frac{b + \sqrt{\Delta}}{2}\right)^2 = -ac + b\,\frac{b + \sqrt{\Delta}}{2}$$

ist, so ist (11) immer die Basis eines Ideals in Ω. Dabei kann die positive Zahl a_{22} willkürlich angenommen werden. Setzen wir $a_{22} = 1$, so ist

(15) $$\lambda = a(x - \omega y)$$

Basisform eines durch (a, b, c) völlig bestimmten Ideals $\mathfrak{a}$, dessen Norm gleich a ist, und eine Basis dieses Ideals ist

(16) $$(a, a\omega).$$

§ 92. Primideale im quadratischen Körper.

Eine Primzahl p ist im quadratischen Körper Ω entweder selbst noch unzerlegbar und ist dann ein Primideal zweiten Grades oder es zerfällt p in zwei Primideale ersten Grades $\mathfrak{p}$, $\mathfrak{p}'$. Wir haben hiernach zwei Fälle zu unterscheiden:

a) $p = \mathfrak{p}$ in Ω unzerlegbar: $N(\mathfrak{p}) = p^2$,

b) $p = \mathfrak{p}\mathfrak{p}'$ $N(\mathfrak{p}) = N(\mathfrak{p}') = p$,

und im letzten Falle können die beiden Primideale $\mathfrak{p}$, $\mathfrak{p}'$ entweder voneinander verschieden oder auch gleich sein, so daß wir noch einen dritten Fall unterscheiden können:

c) $p = \mathfrak{p}^2$, $N(\mathfrak{p}) = p$.

Es handelt sich nun darum, die Bedingungen zu ermitteln, unter denen der eine oder der andere dieser Fälle eintritt.

Wenn $N(\mathfrak{p}) = p$ ist, so ist p die Anzahl der inkongruenten Zahlen (mod $\mathfrak{p}$) in Ω und folglich ist in diesem Fall jede Zahl in Ω einer der rationalen Zahlen r:

(1) $$0, 1, 2, \ldots, p - 1$$

kongruent.

Ist dagegen $N(\mathfrak{p}) = p^2$, so gibt es auch Zahlen, die nach $\mathfrak{p}$ nicht mit einer rationalen Zahl kongruent sind.

Wenn aber $(1, \theta)$ eine Basis von Ω ist und, um beide Fälle von § 90, (9) zu umfassen,

$$\theta = \frac{-\Delta + \sqrt{\Delta}}{2} \tag{2}$$

angenommen wird, so ist im Falle a)

θ nicht kongruent mit einer Zahl r,

im Falle b) oder c)

$$\theta \equiv r \pmod{\mathfrak{p}},$$

wenn man also $-x = 2r + \Delta$ setzt, so folgt:

1. Die notwendige und hinreichende Bedingung für das Eintreten eines der Fälle b), c) ist die, daß es eine rationale ganze Zahl gibt, die mit Δ zugleich gerade oder ungerade ist, für die

$$\frac{x + \sqrt{\Delta}}{2} \equiv 0 \pmod{\mathfrak{p}}. \tag{3}$$

Ist $\mathfrak{p}'$ das mit $\mathfrak{p}$ konjugierte Ideal, so ist

$$\frac{-x + \sqrt{\Delta}}{2} \equiv 0 \pmod{\mathfrak{p}'}, \tag{4}$$

und daraus folgt

$$x^2 \equiv \Delta \pmod{4p}. \tag{5}$$

Ist umgekehrt die Kongruenz (5) durch $x = r$ befriedigt, so ist

$$\frac{r + \sqrt{\Delta}}{2} \cdot \frac{-r + \sqrt{\Delta}}{2} \equiv 0 \pmod{\mathfrak{p}},$$

und folglich genügt entweder $x = r$ oder $x = -r$ der Bedingung (3).

Die beiden Ideale $\mathfrak{p}$, $\mathfrak{p}'$ werden dann miteinander identisch sein, wenn die beiden Zahlen (3) und (4) und folglich auch ihre Summe $\sqrt{\Delta}$ durch $\mathfrak{p}$ und mithin Δ durch p teilbar ist. Dann ist $x \equiv 0$ oder $x \equiv p \pmod{2p}$ die einzige Wurzel von (5).

Wir haben also das Resultat:

2. Der Primfaktor $\mathfrak{p}$ der natürlichen Primzahl p ist vom zweiten Grad, wenn die Kongruenz (5) keine Lösung hat, vom ersten Grad, wenn (5) eine Lösung hat, und p ist das Quadrat von $\mathfrak{p}$, wenn (5) nur eine Lösung hat, wenn also p in Δ aufgeht.

Das letztere ist in Übereinstimmung mit dem allgemeinen Satze Bd. II, § 174.

Mit Benutzung des Symbols (Δ, p), das wir in § 85 eingeführt haben, können wir diesen Sätzen auch die Form geben:

3. Ist $(\Delta, p) = -1$, so ist p unzerlegbar in Ω.
„ $(\Delta, p) = +1$, so zerfällt p in zwei verschiedene konjugierte Primideale.
„ $(\Delta, p) = 0$, so ist p das Quadrat eines Primideals.

§ 93. Darstellung von Zahlen als Idealnormen.

Eine Primzahl p ist nur dann die Norm eines Ideals, wenn $(\Delta, p) = +1$ oder $= 0$ ist, nicht aber, wenn $(\Delta, p) = -1$ ist. Im letzten Falle ist erst p^2 eine Norm, nämlich die von $\mathfrak{p}$. Im allgemeinen kann eine positive ganze rationale Zahl m auf mehrfache Art als Norm dargestellt werden. Wir wollen die Anzahl dieser Darstellungen für den Augenblick mit $\psi(m)$ bezeichnen und näher bestimmen.

Wir nehmen zunächst m als Primzahlpotenz p^k an. Ist dann $(\Delta, p) = +1$ und $p = \mathfrak{p}\mathfrak{p}'$, so kann man p^k in folgender Weise darstellen:

(1) $$p^k = N(\mathfrak{p}^k),\quad N(\mathfrak{p}^{k-1}\mathfrak{p}'),\quad N(\mathfrak{p}^{k-2}\mathfrak{p}'^2),\ \ldots,\ N(\mathfrak{p}'^k),$$

und es ist daher

(2) $$(\Delta, p) = +1:\quad \psi(p^k) = k+1.$$

Ist aber $(\Delta, p) = -1$, so ist, wenn k gerade ist, $p^k = N(p^{\frac{1}{2}k})$, wenn k ungerade ist, p nicht als Norm darstellbar. Es ist also

(3) $$(\Delta, p) = -1:\quad \psi(p^k) = 0 \text{ oder } = 1,$$

je nachdem k ungerade oder gerade ist.

Ist endlich $(\Delta, p) = 0$, also p in Δ enthalten, so ist $p = \mathfrak{p}^2$ und $p^k = N(\mathfrak{p}^k)$; also:

(4) $$(\Delta, p) = 0:\quad \psi(p^k) = 1.$$

Man kann diese drei Fälle in eine Formel zusammenfassen: Die Zahl p^k hat nämlich die folgenden $k+1$ Teiler:

(5) $$1,\ p,\ p^2,\ \ldots,\ p^k.$$

Und daher geben die Formeln (2), (3), (4), wenn $m = p^k$ ist, und n die Teiler von m durchläuft,

(6) $$\psi(m) = \sum^{n} (\Delta, n).$$

Dieser Ausdruck gilt aber allgemein. Denn sind m_1 und m_2 relativ prim und ist

$$m_1 = N(\mathfrak{m}_1), \quad m_2 = N(\mathfrak{m}_2),$$

so ist

$$m = m_1 m_2 = N(\mathfrak{m}_1 \mathfrak{m}_2).$$

Man kann also aus einer Darstellung von m_1, m_2 als Normen eine Darstellung von m als Norm ableiten.

Ist umgekehrt

$$m_1 m_2 = N(\mathfrak{m}) = \mathfrak{m}\mathfrak{m}',$$

wo $\mathfrak{m}$, $\mathfrak{m}'$ konjugierte Ideale sind, so muß, wenn m_1 und m durch ein Primideal $\mathfrak{p}$ teilbar sind, m_1 auch durch $\mathfrak{p}\mathfrak{p}'$ teilbar sein, also ist auch $m_1 = N(\mathfrak{m}_1)$ und ebenso $m_2 = N(\mathfrak{m}_2)$.

Demnach gilt, wenn m_1 und m_2 relativ prim sind:

(7) $$\psi(m_1)\,\psi(m_2) = \psi(m_1 m_2).$$

Andererseits ist, wenn n_1 und n_2 die Teiler von m_1 und m_2 durchlaufen,

$$\Sigma(\Delta, n_1)\,\Sigma(\Delta, n_2) = \Sigma(\Delta, n_1 n_2),$$

und damit ist die Formel (6) allgemein nachgewiesen. Wir sprechen dies als Satz aus:

4. Eine natürliche Zahl m kann in dem quadratischen Körper Ω mit der Grundzahl Δ auf

$$\Sigma(\Delta, n)$$

verschiedene Arten als Norm eines Ideals dargestellt werden, wenn n die sämtlichen Teiler von m durchläuft.

§ 94. Das quadratische Reziprozitätsgesetz.

Aus der Zerlegung der Primzahlen im quadratischen Körper leitet Dedekind einen neuen Beweis des Reziprozitätsgesetzes der quadratischen Reste her [1]).

Nach Bd. II, § 167, 3. ist die notwendige und hinreichende Bedingung dafür, daß das in der Primzahl p aufgehende Primideal $\mathfrak{p}$ (in irgend einem Körper Ω) vom ersten Grade sei, die, daß für jede ganze Zahl ω des Körpers Ω

(1) $$\omega^p \equiv \omega \pmod{\mathfrak{p}},$$

[1]) Dirichlet-Dedekind, Zahlentheorie, 4. Aufl. (S. 636, Anm.).

und dies reduziert sich in unserem Falle des quadratischen Körpers darauf, daß

(2) $$\theta^p \equiv \theta \pmod{\mathfrak{p}}$$

sein muß.

Nehmen wir $\varDelta = -4$, so ist $\theta = i = \sqrt{-1}$ und die Kongruenz (2) wird

$$i^{p-1} \equiv 1 \pmod{\mathfrak{p}}.$$

Da nun $(1 + i)(1 - i) = 2$, also weder 2 noch $(1 \pm i)$ für ein ungerades p durch $\mathfrak{p}$ teilbar sein kann, so muß $i^{p-1} = 1$, also $p - 1$ durch 4 teilbar sein.

Demnach folgt aus § 92, 2.:

1) Die Kongruenz

$$x^2 \equiv -4 \pmod{4p},$$

oder, was dasselbe ist,

$$x^2 \equiv -1 \pmod{p}$$

hat dann und nur dann Lösungen, wenn $p \equiv 1 \pmod{4}$ ist.

Nehmen wir zweitens $\varDelta = 8$, so ist $\theta = \sqrt{2}$, oder, wenn $r = \sqrt{i}$ eine 8te Einheitswurzel ist,

$$\theta = r + r^{-1},$$

und die Bedingung (2) läßt sich nach dem binomischen Satze so darstellen:

$$r^p + r^{-p} \equiv r + r^{-1} \pmod{\mathfrak{p}}.$$

Dies fordert:

$$(r^p - r)(r^p - r^{-1})\, r^{-p} \equiv 0 \pmod{\mathfrak{p}},$$

also:

$$r^p \equiv r \text{ oder } r^p \equiv r^{-1} \pmod{\mathfrak{p}},$$

$$r^{p \pm 1} \equiv 1, \quad i^{\frac{p \pm 1}{2}} - 1 \equiv 0 \pmod{\mathfrak{p}},$$

und daraus folgt wie oben für ein ungerades p:

$$p \equiv \pm 1 \pmod{8}.$$

2) Die Kongruenz

$$x^2 \equiv 2 \pmod{p}$$

ist also dann und nur dann lösbar, wenn $p \equiv 1$ oder $p \equiv -1 \pmod{8}$ ist.

Endlich setzen wir, wenn q eine ungerade Primzahl ist,

(3) $$\varDelta = \pm q$$

und bestimmen das Vorzeichen so, daß $\pm q \equiv 1 \pmod 4$ wird. Es ist in diesem Falle

$$\theta = \frac{-1 + \sqrt{\pm q}}{2},$$

und diesen Ausdruck können wir durch $q$te Einheitswurzeln darstellen. Es bedeute r eine imaginäre $q$te Einheitswurzel und es durchlaufe a die quadratischen Reste, b die Nichtreste von q. Wir setzen, wie in Bd. I, § 179

$$(4) \qquad A = \sum^{a} r^{a}, \quad B = \sum^{b} r^{b}$$

und haben nach den dortigen Formeln (3), die ohne Benutzung des Reziprozitätsgesetzes abgeleitet sind:

$$(5) \qquad \theta = A, \qquad \theta' = B.$$

Das Vorzeichen von $\sqrt{\pm q}$ hängt von der Wahl von r ab, kommt aber hier nicht in Betracht. Nun ist nach dem polynomischen Lehrsatz:

$$A^p \equiv \Sigma r^{pa}, \quad B^p \equiv \Sigma r^{pb},$$

also

$$A^p \equiv A, \quad B^p \equiv B, \quad \text{wenn} \left(\frac{p}{q}\right) = +1,$$

und

$$A^p \equiv B, \quad B^p \equiv A, \quad \text{wenn} \left(\frac{p}{q}\right) = -1.$$

Da A nicht kongruent B ist, wenn p von q verschieden ist, so folgt hieraus und aus 2. des vorigen Paragraphen:

3) Die Kongruenz

$$x^2 \equiv \pm q \pmod p$$

hat dann und nur dann Lösungen, wenn p quadratischer Rest von q ist.

Und dies ist das Reziprozitätsgesetz mit seinen Ergänzungssätzen.

§ 95. Äquivalente Formen und Ideale im quadratischen Körper.

Wenn die beiden Ideale [§ 91, (16)]

$$(1) \qquad \mathfrak{a} = (a, a\,\omega), \quad \mathfrak{a}' = (a', a'\,\omega')$$

äquivalent sind, so gibt es eine (ganze oder nicht ganze) Zahl η in Ω, für die $\eta\,\mathfrak{a}' = \mathfrak{a}$ ist, und diese Zahl η ist durch die Ideale $\mathfrak{a}, \mathfrak{a}'$ selbst bis auf einen Faktor, der eine numerische Einheit

ist, bestimmt. Es muß also vier ganze rationale Zahlen $\alpha, \beta, \gamma, \delta$ geben, die der Bedingung

$$(2) \quad \begin{aligned} \eta a' &= a(\alpha - \gamma\omega), \\ \eta a'\omega' &= a(-\beta + \delta\omega) \end{aligned}$$

genügen. Bezeichnen wir für den Augenblick mit $\eta_1, \omega_1, \omega_1'$ die zu η, ω, ω' konjugierten Zahlen, so ist hiernach

$$a'^2\eta\eta_1 \begin{vmatrix} 1, \omega' \\ 1, \omega_1' \end{vmatrix} = a^2 \begin{vmatrix} \alpha, -\gamma \\ -\beta, \delta \end{vmatrix} \begin{vmatrix} 1, \omega \\ 1, \omega_1 \end{vmatrix},$$

also:

$$a'^2\eta\eta_1(\omega' - \omega_1') = a^2(\alpha\delta - \beta\gamma)(\omega - \omega_1),$$

und da nach § 91, (12):

$$a(\omega - \omega_1) = a'(\omega' - \omega_1') = -\sqrt{\Delta}$$

ist, so folgt hieraus, wenn

$$\varepsilon = \alpha\delta - \beta\gamma$$

gesetzt wird,

$$(3) \quad a\varepsilon = a'\eta\eta_1;$$

wenn also, wie wir schon angenommen haben, a und a' positiv sind und (nach dem verschärften Äquivalenzbegriff) $\eta\eta_1$ positiv ist, so ist auch ε positiv.

Vertauschen wir aber $\mathfrak{a}$ mit $\mathfrak{a}'$, so geht η in $1:\eta$ über und ε mag in ε' übergehen. Demnach folgt auch

$$(4) \quad a'\varepsilon' = \frac{a}{\eta\eta_1},$$

und folglich $\varepsilon\varepsilon' = 1$. Da aber ε und ε' positive ganze rationale Zahlen sind, so folgt hieraus $\varepsilon = \varepsilon' = 1$. Also nach (2)

$$(5) \quad \omega' = \frac{-\beta - \delta\omega}{\alpha - \gamma\omega}, \quad \omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}, \quad \alpha\delta - \beta\gamma = 1.$$

Nun sind ω und ω' die Wurzeln der beiden Formen

$$(a, b, c), \quad (a', b', c') \quad [\S\ 91, (13)],$$

und durch (5) ist die Äquivalenz dieser Formen ausgedrückt. Wir haben daher, übereinstimmend mit der allgemeinen Theorie (§ 88) den Satz:

5. Die zu äquivalenten Idealen gehörigen quadratischen Formen sind äquivalent.

Man erkennt hieraus die Bedeutung des verschärften Äquivalenzbegriffes: Wollte man nämlich auch negative Werte von $N(\eta)$ zulassen, so könnten auch $\varepsilon = -1$ und die entsprechenden Formen uneigentlich äquivalent sein.

Es seien nun umgekehrt $\varphi = (a, b, c)$, $\varphi' = (a', b', c')$ zwei äquivalente Formen mit positiven ersten Koeffizienten a, a', und

$$(6) \qquad \omega = -\frac{b + \sqrt{\Delta}}{2a}, \quad \omega' = -\frac{b' + \sqrt{\Delta}}{2a'}.$$

Dann gibt es eine lineare Substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ mit der Determinante $+1$, durch die (a, b, c) in (a', b', c') übergeht.

Es ist dann

$$(7) \qquad \begin{aligned} a' &= a\alpha^2 + b\alpha\gamma + c\gamma^2, \\ b' &= 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta, \\ c' &= a\beta^2 + b\beta\delta + c\delta^2, \end{aligned}$$

$$(8) \qquad \omega = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta}, \quad \omega' = \frac{\delta\omega - \beta}{-\gamma\omega + \alpha},$$

und eine kleine Rechnung zeigt, daß ω und ω' entsprechende Wurzeln, d. h. Wurzeln mit dem gleichen Vorzeichen von $\sqrt{\Delta}$ sind.

Demnach erhalten wir für die zu φ und φ' gehörigen Ideale $\mathfrak{a}, \mathfrak{a}'$ zwei Basisformen:

$$\begin{aligned} \lambda &= a(x - \omega y), \\ \lambda' &= a'(x' - \omega' y'), \end{aligned}$$

und nach (8) ist

$$\lambda = \frac{a[(\delta x - \beta y) + (\gamma x - \alpha y)\omega']}{\gamma\omega' + \delta}.$$

Setzt man also

$$x' = \delta x - \beta y, \quad y' = -\gamma x + \alpha y,$$

so folgt

$$\lambda = \frac{a}{a'(\gamma\omega' + \delta)} \lambda',$$

da $a : a'(\gamma\omega' + \delta)$ eine Zahl in Ω ist, so folgt, daß $\mathfrak{a}$ und $\mathfrak{a}'$ äquivalent sind.

Wir haben also wieder in Übereinstimmung mit dem allgemeinen Satz § 88, 4. und zugleich in näherer Bestimmung:

6. Sind (a, b, c) (a', b', c') zwei äquivalente Formen mit positiven ersten Koeffizienten, und sind ω, ω' entsprechende Wurzeln dieser Formen, so sind die Ideale $(a, a\omega)$ und $(a', a'\omega')$ äquivalent.

Bei negativer Diskriminante haben die ersten Koeffizienten äquivalenter Formen immer dasselbe Vorzeichen, und man berücksichtigt nur die Formen, in denen dieses Vorzeichen positiv ist.

Bei positiver Diskriminante gibt es in jeder Formklasse Formen mit positiven ersten Koeffizienten, und daher entsprechen sich Formenklassen und Idealklassen in eindeutiger Weise.

Eine Basis des Hauptideals η ist $(\eta, \eta\,\theta)$ und

$$\begin{aligned} \theta &= \frac{\sqrt{\Delta}}{2}, & \theta^2 &= \frac{\Delta}{4}, & \Delta &\equiv 0 \\ \theta &= \frac{-1+\sqrt{\Delta}}{2}, & \theta^2 &= \frac{\Delta-1}{4} - \theta, & \Delta &\equiv 1 \end{aligned} \pmod 4.$$

Sind x, y ganze rationale Zahlen und

$$\eta = x + y\,\theta,$$

so ist diese Basis in den beiden Fällen:

$$\begin{aligned} (\alpha_1, \alpha_2) &= \left(x + y\,\theta,\ \ \frac{\Delta\,y}{4} + \theta\,x\right), \\ &= \left(x + y\,\theta,\ \ y\,\frac{\Delta-1}{4} + (x-y)\,\theta\right) \end{aligned}$$

und die Substitutionsdeterminante A [§ 87, (1)] ist

$$x^2 - \frac{\Delta}{4}\,y^2,\quad x^2 - x\,y + \frac{1-\Delta}{4}\,y^2 = N(\eta).$$

Die Basis (α_1, α_2) ist also positiv, wenn die Norm von η positiv ist (sonst müßte α_1 mit α_2 vertauscht werden). Aus der Basisform

$$\lambda = \alpha_1\,t_1 + \alpha_2\,t_2 = \eta\,(t_1 + \theta\,t_2)$$

erhält man

$$N(\lambda) = N(\eta)\,T,$$

und danach wird T die Hauptform

(9) $$\left(1,\ 0,\ \frac{\Delta}{4}\right),\quad \left(1,\ -1,\ \frac{+1-\Delta}{4}\right).$$

Wäre $N(\eta)$ negativ, so würde man für T die Formen

$$\left(-1,\ 0,\ \frac{-\Delta}{4}\right),\quad \left(-1,\ +1\ \frac{-1-\Delta}{4}\right)$$

erhalten haben, und diese sind mit (9) nur dann äquivalent, wenn die Pellsche Gleichung $t^2 - \Delta\,u^2 = -4$ lösbar ist.

Zwölfter Abschnitt.

Ordnungen im quadratischen Körper[1]).

§ 96. Diskriminanten der Ordnungen.

1. Definition. Ist Q eine natürliche Zahl, so heißt die Gesamtheit der ganzen Zahlen des quadratischen Körpers Ω, die nach dem Modul Q mit einer rationalen Zahl kongruent sind, eine Ordnung, und Q heißt der Führer dieser Ordnung.

Die Ordnung mit dem Führer Q wird mit $[Q]$ bezeichnet.

Es ergibt sich aus dieser Definition:

1. Alle rationalen ganzen Zahlen gehören jeder Ordnung an;

2. Summe, Differenz und Produkt zweier Zahlen der Ordnung gehören derselben Ordnung an;

d. h. man kann innerhalb der Ordnung Addition, Subtraktion und Multiplikation unbedingt ausführen, nicht aber allgemein die Division.

Die Gesamtheit aller ganzen Zahlen des Körpers Ω bilde gleichfalls eine Ordnung (vom Führer 1), die Hauptordnung, die also mit [1] zu bezeichnen wäre.

---

[1]) Dedekind hat den Ausdruck Ordnung in der allgemeinen Theorie der algebraischen Zahlen eingeführt, weil sie in dem besonderen Fall des quadratischen Körpers den Gaussschen Ordnungen der quadratischen Formen entsprechen. Hilbert gebraucht dafür den Ausdruck „Ring" oder „Zahlring". Vgl. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie (§ 172 der dritten, § 170 der vierten Auflage). Dedekind: Über die Anzahl der Idealklassen in den verschiedenen Ordnungen eines endlichen Körpers, Festschrift zur Säkularfeier von Gauss' Geburtstag, Braunschweig 1877. Hilbert: Die Theorie der algebraischen Zahlen, Bericht der Deutschen Mathematischen Vereinigung von 1894/95, Kap. IX.

Wir setzen, wenn Δ die Grundzahl des Körpers Ω ist, je nachdem Δ gerade oder ungerade ist:

$$(1)\qquad \theta_0 = \tfrac{1}{2}\sqrt{\Delta}, \qquad \text{oder} \qquad \theta_0 = \frac{-1+\sqrt{\Delta}}{2}.$$

Dann ist nach § 90 jede ganze Zahl des Körpers Ω in der Form

$$(2)\qquad \omega = x + y\,\theta_0$$

darstellbar, worin x und y ganze Zahlen sind, und diese Zahl ist dann und nur dann nach dem Modul Q mit einer rationalen Zahl a kongruent, wenn y durch Q teilbar ist, weil dann

$$\frac{x - a + y\,\theta_0}{Q}$$

eine ganze Zahl sein muß. Demnach sind alle Zahlen der Ordnung $[Q]$ in der Form enthalten:

$$\omega = x + y\,Q\,\theta_0,$$

oder in den beiden in (1) unterschiedenen Fällen, wenn

$$(3)\qquad D = Q^2\Delta$$

gesetzt wird:

$$(4)\qquad \begin{aligned} & x - y\frac{\sqrt{D}}{2}, && \Delta \text{ gerade},\\ & x - \frac{Q}{2}\,y + y\,\frac{\sqrt{D}}{2}, && \Delta \text{ ungerade, } D \text{ gerade},\\ & x - \frac{Q-1}{2}\,y + y\,\frac{-1+\sqrt{D}}{2}, && D \text{ ungerade}. \end{aligned}$$

Setzen wir also

$$(5)\qquad \begin{aligned} \theta &= \frac{\sqrt{D}}{2}, && D \equiv 0 \pmod 4\\ \theta &= \frac{-1+\sqrt{D}}{2}, && D \equiv 1 \pmod 4 \end{aligned}$$

und ersetzen in den beiden letzten Formeln (4) die willkürlich ganzen Zahlen

$$x - \frac{Q}{2}y, \quad x - \frac{Q-1}{2}y$$

durch x, so erhalten wir das Resultat:

2. Satz. Jede Zahl der Ordnung $[Q]$ und nur diese sind in der Form enthalten

(6) $$\omega = x + y\theta,$$

worin x, y beliebige ganze rationale Zahlen sind.

Wir nennen das System

(7) $$(1, \theta)$$

eine Basis der Ordnung $[Q]$.

Durch Einsetzen von (5) kann man die Zahlen (6) auch in der Form darstellen:

(8) $$\omega = \frac{x + y\sqrt{D}}{2},$$

wobei die x, y ganze Zahlen sind, die der Bedingung genügen

(9) $$x^2 - y^2 D \equiv 0 \pmod 4.$$

Die Zahl D ist eine Diskriminante, deren Stamm Δ ist. Wir nennen sie die Diskriminante der Ordnung $[Q]$.

§ 97. Ordnungen und Ideale.

Es sei $\mathfrak{m}$ ein Ideal des quadratischen Körpers Ω. Wenn alle durch $\mathfrak{a}$ teilbaren ganzen Zahlen durch eine rationale Zahl m teilbar sind, so ist das Ideal $\mathfrak{a} = m\mathfrak{m}$ durch m teilbar; es ist

$$N(\mathfrak{a}) = m^2 N(\mathfrak{m}),$$

und die rationale Zahl $mN(\mathfrak{m})$, die kleiner ist als $N(\mathfrak{a})$, ist durch $\mathfrak{a}$ teilbar.

Ist m die größte natürliche Zahl, durch die $\mathfrak{a}$ teilbar ist, so wollen wir m den Teiler von $\mathfrak{a}$ nennen. Ist der Teiler $= 1$, so heißt das Ideal primär, sonst abgeleitet. Man erhält alle aus einem primären Ideal $\mathfrak{m}$ abgeleiteten Ideale, indem man $\mathfrak{m}$ mit beliebigen natürlichen Zahlen multipliziert, und alle aus einem primären Ideal abgeleiteten Ideale sind untereinander äquivalent.

3. Satz. Ist $\mathfrak{a}$ ein primäres Ideal, so ist die Norm von $\mathfrak{a}$ zugleich die kleinste durch $\mathfrak{a}$ teilbare natürliche Zahl.

Bezeichnen wir nämlich die kleinste durch $\mathfrak{a}$ teilbare natürliche Zahl mit a, so ist die Norm von $\mathfrak{a}$ jedenfalls durch a teilbar. Wir setzen

$$N(\mathfrak{a}) = ma,$$

und wenn $\mathfrak{a}'$ das zu $\mathfrak{a}$ konjugierte Ideal ist, so ergibt sich, da nach Bd. II, § 164 die Norm eines Ideals gleich dem Produkt der konjugierten Ideale ist,

(1) $$N(\mathfrak{a}) = \mathfrak{a}\mathfrak{a}' = ma.$$

Da a durch $\mathfrak{a}$ teilbar sein soll, so setzen wir

$$a = \mathfrak{a}\mathfrak{m}' = \mathfrak{a}'\mathfrak{m}$$

und erhalten aus (1):

$$\mathfrak{a} = m\mathfrak{m}. \tag{2}$$

Also geht m im Teiler des Ideals $\mathfrak{a}$ auf, und damit ist der Satz 3. bewiesen, da, wenn $\mathfrak{a}$ primär ist, sein Teiler $= 1$ sein muß.

4. Satz. Ist $\mathfrak{m}$ ein primäres Ideal des Körpers Ω, so ist jede ganze Zahl in Ω nach dem Modul $\mathfrak{m}$ mit einer rationalen Zahl kongruent.

Nach Bd. II, § 165 ist nämlich allgemein $N(\mathfrak{m})$ die Anzahl der nach $\mathfrak{m}$ inkongruenten Zahlen in Ω. Ist nun $N(\mathfrak{m}) = a$ zugleich die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl, so sind die a Zahlen

$$0, 1, 2, \ldots, a-1$$

alle inkongruent, und darunter sind alle Zahlklassen modulo $\mathfrak{m}$ vertreten.

Es sei jetzt $[Q]$ eine Ordnung mit dem Führer Q und der Diskriminante D und $(1, \theta)$ die Basis dieser Ordnung. Ferner sei $\mathfrak{m}$ ein primäres zu Q teilerfremdes Ideal. Nach dem Satz 4. gibt es dann eine ganze rationale Zahl t, die der Bedingung

$$\theta + t \equiv 0 \pmod{\mathfrak{m}}$$

genügt. Wir setzen

$$\begin{aligned} t &= \frac{b}{2}, && \text{wenn } D \equiv 0 \\ t &= \frac{1+b}{2}, && \;\text{„}\;\; D \equiv 1 \end{aligned} \pmod 4 \tag{3}$$

ist, und erhalten nach § 96, (5):

$$\theta + t = \frac{b + \sqrt{D}}{2} \equiv 0 \pmod{\mathfrak{m}}, \tag{4}$$

worin b eine ganze rationale Zahl ist, die nach (3) der Bedingung

$$b \equiv D \pmod 2$$

genügt. Außerdem sei

$$N(\mathfrak{m}) = a, \tag{5}$$

also a die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl.

Durch die Kongruenz (4) ist die Zahl b nur nach dem Modul $2a$ bestimmt. Denn sind b, b' zwei Zahlen, die der Bedingung (4) genügen, so ist $\frac{1}{2}(b' - b)$ durch a teilbar.

Da ferner

$$N\left(\frac{b + \sqrt{D}}{2}\right) = \frac{b^2 - D}{4}$$

eine durch $\mathfrak{m}$ teilbare ganze rationale Zahl ist, so muß sie durch a teilbar sein; setzen wir sie $= ac$, so ist c eine ganze rationale Zahl und

$$D = b^2 - 4ac, \tag{6}$$

$$b^2 \equiv D \pmod{4a}, \tag{7}$$

und wenn die Kongruenz (7) erfüllt ist, so genügt auch jede mit b nach dem Modul $2a$ kongruente Zahl b' derselben Kongruenz.

Wir schließen hieraus:

5. Satz. Jedes primäre zu Q teilerfremde Ideal $\mathfrak{m}$, dessen Norm $= a$ ist, liefert uns durch (4) eine und nur eine Wurzel b der Kongruenz (7), wenn als Wurzeln nicht einzelne Zahlen, sondern Zahlklassen nach dem Modul $2a$ betrachtet werden.

Die beiden Zahlen

$$a, \quad \frac{b + \sqrt{D}}{2} \tag{8}$$

können, wenn a relativ prim zu Q ist, nicht beide durch eine und dieselbe rationale Primzahl teilbar sein; denn sonst müßte

$$\frac{b + \sqrt{D}}{2} - \frac{b - \sqrt{D}}{2} = \sqrt{D}$$

durch p teilbar sein; also wäre D durch p^2 teilbar und p müßte ein Teiler von Q sein, gegen die Voraussetzung.

Für ein ungerades p ist dies evident, für $p = 2$ aber würde folgen:

$$b \equiv 0 \pmod{2}, \quad b^2 - D \equiv 0 \pmod{16},$$

und mithin

$$D \equiv 0, 4 \pmod{16}.$$

Es wäre also $D/4$ noch Diskriminante und 2 müßte in Q aufgehen. Damit ist bewiesen:

6. Satz. Ist a eine zu Q teilerfremde natürliche Zahl und b eine Wurzel von (7), so erhält man ein bestimmtes primäres Ideal $\mathfrak{m}$ als größten gemeinschaftlichen Teiler der beiden Zahlen (8).

Jetzt beweisen wir:

7. Satz. Jede durch das primäre Ideal $\mathfrak{m}$ teilbare, zu Q teilerfremde Zahl μ der Ordnung $[Q]$ ist in der Form

$$\mu = ax + \frac{b + \sqrt{D}}{2}y \tag{9}$$

einmal und nur einmal darstellbar, wenn x, y ganze rationale Zahlen sind. Werden x, y als Variable be-

trachtet, so heißt μ eine Basisform des Ideals $\mathfrak{m}$ in der Ordnung $[Q]$.

Zum Beweis bemerken wir, daß jede Zahl der Ordnung $[Q]$ wegen (4) in der Form enthalten ist

$$\omega = z + \frac{b + \sqrt{D}}{2} y, \tag{10}$$

wenn y und z ganze rationale Zahlen sind. Ist nun $\mathfrak{m}$ primär, so ist

$$N(\mathfrak{m}) = a \tag{11}$$

die kleinste durch $\mathfrak{m}$ teilbare natürliche Zahl, und wenn also ω durch $\mathfrak{m}$ teilbar sein soll, so muß z durch a teilbar sein. Wenn wir also $z = ax$ setzen, so erhalten wir die Form (9). Umgekehrt ist evident, daß jede Zahl dieser Form durch $\mathfrak{m}$ teilbar ist.

Daß die Darstellung einer Zahl μ nur auf eine Art in dieser Form möglich ist, folgt daraus, daß $\sqrt{D}$ irrational ist.

Die Form μ heißt daher eine Basisform des Ideals $\mathfrak{m}$ in der Ordnung Q. Man erhält daraus eine Basisform desselben Ideals im Körper Ω:

$$\lambda = ax + \frac{b' + \sqrt{\Delta}}{2} y,$$

wenn b' aus der Kongruenz

$$b' Q \equiv b \pmod{2a}$$

bestimmt wird, die immer lösbar ist, da Q relativ prim zu a, und bei geradem Q auch b gerade ist.

Aus (9) ergibt sich

$$N(\mu) = a(ax^2 + bxy + cy^2). \tag{12}$$

Die Zahl μ, die man erhält, wenn man in (9) für x, y bestimmte Zahlen setzt, können wir in Idealfaktoren zerlegen:

$$\mu = \mathfrak{a}\mathfrak{m},$$

wenn

$$N(\mathfrak{a}) = ax^2 + bxy + cy^2 \tag{13}$$

ist, und es gilt der Satz:

8. Satz. Ist μ relativ prim zu Q, und haben x, y keine gemeinschaftlichen Teiler, so ist das Ideal $\mathfrak{a}$ primär.

Wir beweisen ihn so: Es sei p eine in $\mathfrak{a}$ aufgehende rationale Primzahl; dann ist μ durch p teilbar und daraus folgt zunächst, daß y durch p teilbar sein muß; denn eine Zahl ω von der Form (10) kann nur dann durch eine in Q nicht aufgehende Primzahl p teilbar sein, wenn sowohl y als $z = ax$ durch p teilbar sind. Demnach kann, da nach Voraussetzung x und y

relativ prim sind, x nicht durch p teilbar sein, und es muß a durch p teilbar sein.

Setzen wir $a = p^k a_1$, wo a_1 nicht mehr durch p teilbar ist, und bezeichnen mit $\mathfrak{p}$ ein in p aufgehendes Primideal, so muß wegen (11) $\mathfrak{p}$ in $\mathfrak{m}$ oder in $\mathfrak{m}'$ aufgehen, und da $\mathfrak{m}$ primär vorausgesetzt war, kann $\mathfrak{p}$ nicht $= p$ sein. Es ist daher $N(\mathfrak{p}) = p = \mathfrak{p}\mathfrak{p}'$, und wenn $\mathfrak{m}$ durch $\mathfrak{p}$ teilbar ist, kann es nicht zugleich durch $\mathfrak{p}'$ teilbar sein. Folglich ist $\mathfrak{m}$ durch $\mathfrak{p}^k$ teilbar. Es ist also nach der Definition von $\mathfrak{m}$ (Satz 6) auch $\frac{b+\sqrt{D}}{2}$ durch $\mathfrak{p}^k$ teilbar, folglich $\frac{b+\sqrt{D}}{2}\,y$ mindestens durch $\mathfrak{p}^{k+1}$, und ax und folglich μ genau durch $\mathfrak{p}^k$, während andererseits $\mathfrak{a}\mathfrak{m} = \mu$ gleichfalls mindestens durch $\mathfrak{p}^{k+1}$ teilbar ist, worin ein Widerspruch liegt. Ähnliches gilt auch, wenn $p = \mathfrak{p}^2$ ist, also in $\varDelta$ (aber nicht in Q) aufgeht. Folglich kann in $\mathfrak{a}$ keine rationale Primzahl enthalten sein und $\mathfrak{a}$ ist primär.

Nach dem, was bisher bewiesen ist, können wir noch folgenden Satz formulieren:

9. Satz. Sind

$$\mu = ax + \frac{b+\sqrt{D}}{2}y = \mathfrak{m}\mathfrak{a},$$

$$\mu' = ax' + \frac{+\sqrt{D}}{2}y' = \mathfrak{m}\mathfrak{a}'$$

zwei zu Q teilerfremde Zahlen, haben weder x und y noch x' und y' einen gemeinschaftlichen Teiler, ist

$$N(\mathfrak{a}) = N(\mathfrak{a}') = A,$$

und für eine und dieselbe Zahl B

$$\begin{aligned}\frac{B+\sqrt{D}}{2} &\equiv 0 \pmod{\mathfrak{a}}\\ &\equiv 0 \pmod{\mathfrak{a}'},\end{aligned}$$

so sind die beiden Ideale $\mathfrak{a}$ und $\mathfrak{a}'$ identisch, und die Zahlen μ, μ' unterscheiden sich nur durch einen Einheitsfaktor.

Denn $\mathfrak{a}$ sowohl als $\mathfrak{a}'$ sind nach 8. primär und sind nach 6. definiert als größter gemeinschaftlicher Teiler von

$$A \quad \text{und} \quad \frac{B+\sqrt{D}}{2}.$$

Dreizehnter Abschnitt.

Äquivalenz nach Zahlgruppen.

§ 98. Zahlgruppen in den Ordnungen.

Um die Beziehungen der quadratischen Irrationalzahlen zu den Ordnungen der quadratischen Formen genauer zu erforschen, leiten wir aus den Zahlen des Körpers Ω Zahlgruppen nach folgenden Gesichtspunkten ab.

1. Wir nehmen eine beliebige natürliche Zahl Q und schließen von den ganzen Zahlen in Ω zunächst alle die aus, die nicht teilerfremd zu Q sind. Von den übrigen nehmen wir auch noch beliebige Quotienten.

Die so erhaltenen ganzen und gebrochenen Zahlen η nennen wir fremd gegen Q. Ihre Gesamtheit sei mit O bezeichnet. Sie bilden insofern eine Gruppe, als Multiplikation und Division zweier dieser Zahlen immer Zahlen desselben Systems liefern.

2. Wir verfahren nun ebenso mit den Zahlen der Ordnung $[Q]$, d. h. wir schließen alle Zahlen dieser Ordnung, die mit Q nicht relativ prim sind, aus und bilden auch noch die Quotienten beliebiger zweier der übrig gebliebenen Zahlen. Wir bezeichnen diese Zahlen in η' und ihre Gesamtheit mit O', und nennen sie ganze und gebrochene Zahlen der Ordnung $[Q]$. Die Zahlen O' sind alle in O enthalten und bilden gleichfalls der Multiplikation und Division gegenüber eine Gruppe. Wir nennen sie die Gruppe der Ordnung $[Q]$ oder kurz eine Ordnungsgruppe.

Jede Zahl η in O kann durch Multiplikation mit einer ganzen rationalen zu Q teilerfremden Zahl n in eine ganze Zahl ω verwandelt werden.

Wenn η' eine Zahl in O' ist, so kann man den Nenner rational machen und findet, daß $n\eta'$ eine ganze Zahl der Ordnung $[Q]$ und folglich mit einer rationalen Zahl nach dem Modul Q kongruent ist.

Da n teilerfremd zu Q ist, so kann man diese Zahl $= nr$ setzen, worin r eine zu Q teilerfremde rationale Zahl ist. Demnach hat jede Zahl η' die Eigenschaft

$$\eta' \equiv r \pmod{Q}, \tag{1}$$

worin r eine ganze rationale Zahl und die Kongruenz in dem Sinne $n\eta' \equiv nr$ zu verstehen ist.

Die Kongruenzen (1) lassen sich multiplizieren und dividieren, wenn man unter r^{-1} die der Bedingung $r \,.\, r^{-1} \equiv 1 \pmod{Q}$ genügende ganze Zahl versteht.

Umgekehrt gehört eine ganze oder gebrochene Zahl η', die einer Bedingung (1) genügt, der Gruppe O' an. Denn ist $n\eta' = \omega \equiv nr$ eine Zahl in $[Q]$, so ist $\eta' = \omega : n$ ein Quotient zweier solcher Zahlen.

3. In O' ist nun wieder eine Gruppe O_0 enthalten, die aus allen Zahlen η_0 besteht, die der Bedingung

$$\eta_0 \equiv 1 \pmod{Q} \tag{2}$$

genügen, und die Zahlen von O_0 ergeben durch Multiplikation und Division gleichfalls wieder Zahlen von O_0.

Wir haben also dreierlei Zahlgruppen, deren jede in der vorangehenden enthalten ist:

1. O enthält alle gegen Q fremden Zahlen in Ω.
2. O' enthält die gegen Q fremden ganzen und gebrochenen Zahlen der Ordnung $[Q]$.
3. O_0 enthält die Zahlklassen in O', die nach dem Modul Q mit der Einheit kongruent sind.

Die Gruppen O, O', O_0 sind unendliche Abelsche Gruppen. Nimmt man aber ein volles Restsystem rationaler, zu Q teilerfremder Zahlen $r_1, r_2, \ldots, r_\mu$, so kann jede Zahl in O' als Produkt eines dieser r_i mit einer Zahl in O_0 dargestellt werden, und man kann daher nach der in Bd. II, § 2 gebrauchten Ausdrucksweise setzen:

$$O' = r_1 O_0 + r_2 O_0 + \cdots + r_\mu O_0, \tag{3}$$

und μ ist der Index des Teilers O_0 von O:

$$\mu = (O', O_0), \tag{4}$$

also eine endliche Zahl, nämlich:

$$\mu = \varphi(Q) = Q\,\Pi\left(1 - \frac{1}{q}\right), \tag{5}$$

worin $\varphi(Q)$ das in der Zahlentheorie gebräuchliche Zeichen für die Anzahl der Zahlklassen nach dem Modul Q mit zu Q teiler-

fremden Zahlen bedeutet und q in dem Produkt Π die voneinander verschieden in Q aufgehenden Primzahlen durchläuft.

Bezeichnen wir mit

$$\varrho_1, \varrho_2, \ldots, \varrho_\nu$$

ein volles Repräsentantensystem der zu Q teilerfremden Zahlen in Ω, nach dem Modul Q genommen, so ist in gleicher Weise

$$O = \varrho_1 O_0 + \varrho_2 O_0 \cdots + \varrho_\nu O_0 \tag{6}$$

und

$$\nu = \psi(Q) = (O, O_0) \tag{7}$$

ist der Index des Teilers O_0 in bezug auf O.

Die Zahl $\psi(Q)$ haben wir in § 168, (3) des II. Bandes allgemein bestimmt, auch für den Fall, daß an Stelle von Q ein Ideal tritt. Da nun hier $N(Q) = Q^2$ ist, so haben wir:

$$\psi(Q) = Q^2 \Pi\left(1 - \frac{1}{N(\mathfrak{q})}\right), \tag{8}$$

wenn $\mathfrak{q}$ die voneinander verschiedenen idealen Primteiler von Q durchläuft.

Nun ist (§ 92)

1. $N(\mathfrak{q}) = q$, wenn $(\Delta, q) = 0$,
2. $N(\mathfrak{q}) = q$, wenn $(\Delta, q) = +1$,
3. $N(\mathfrak{q}) = q^2$, wenn $(\Delta, q) = -1$.

Wir wollen diese dreierlei Primzahlen mit q_1, q_2, q_3 bezeichnen und bemerken, daß jede Primzahl q_2 die Norm von zwei verschiedenen Primidealen $\mathfrak{q}$ ist. Demnach ergibt sich aus (8)

$$\psi(Q) = Q^2 \Pi\left(1 - \frac{1}{q_1}\right) \Pi\left(1 - \frac{1}{q_2}\right)^2 \Pi\left(1 - \frac{1}{q_3^2}\right). \tag{9}$$

Nun ist der Index von O' in bezug auf O nach Bd. II, § 2 (4):

$$j = \frac{\nu}{\mu} = (O, O') = \frac{(O, O_0)}{(O', O_0)} = \frac{\psi(Q)}{\varphi(Q)}$$

und

$$\varphi(Q) = Q \Pi\left(1 - \frac{1}{q_1}\right) \Pi\left(1 - \frac{1}{q_2}\right) \Pi\left(1 - \frac{1}{q_3}\right);$$

folglich ergibt sich:

$$(O, O') = Q \Pi\left(1 - \frac{1}{q_2}\right) \Pi\left(1 + \frac{1}{q_3}\right),$$

wofür dann auch gesetzt werden kann (nach 1., 2., 3.):

$$j = (O, O') = Q \Pi\left(1 - \frac{(\Delta, q)}{q}\right). \tag{10}$$

Darin bezieht sich das Produkt Π auf alle in Q aufgehenden Primzahlen q.

Wir können also ein Repräsentantensystem

$$\sigma_1, \sigma_2, \ldots, \sigma_j$$

in O so auswählen, daß

$$O = \sigma_1 O' + \sigma_2 O' + \cdots \sigma_j O' \tag{11}$$

wird.

§ 99. Äquivalenz in den Ordnungen.

10. Definition. Wir wollen jetzt zwei Ideale $\mathfrak{a}, \mathfrak{a}'$ äquivalent nach der Ordnung $[Q]$ nennen, wenn

$$\mathfrak{a}' = \eta' \mathfrak{a} \tag{1}$$

ist, und η' eine Zahl in O' bedeutet. $\mathfrak{a}$ und $\mathfrak{a}'$ werden dabei immer zu Q teilerfremd vorausgesetzt.

Nimmt man eine durch $\mathfrak{a}$ teilbare Zahl $\mu = \mathfrak{a}\mathfrak{m}$ in $[Q]$ so an, daß $\mathfrak{m}$ ein primäres Ideal wird, und setzt $\mu' = \eta'\mu$, so wird:

$$\begin{aligned} \mu &= \mathfrak{m}\mathfrak{a}, \\ \mu' &= \mathfrak{m}\mathfrak{a}', \end{aligned} \tag{2}$$

und wir können die Äquivalenz von $\mathfrak{a}$ und $\mathfrak{a}'$ nach $[Q]$ auch dadurch erklären, daß $\mathfrak{a}$ und $\mathfrak{a}'$ durch Multiplikation mit einem und demselben Ideal $\mathfrak{m}$ in Zahlen der Ordnung $[Q]$ verwandelt werden.

Durch das Ideal $\mathfrak{m}$ ist nach § 97 eine Schar paralleler quadratischer Formen (a, b, c) bestimmt[1]), in der a und b aus

$$a = N(\mathfrak{m}), \quad \frac{b + \sqrt{D}}{2} \equiv 0 \pmod{\mathfrak{m}} \tag{3}$$

bestimmt wird. Und diese Formenschar ändert sich also nach (2) nicht, wenn $\mathfrak{a}$ durch ein äquivalentes Ideal $\mathfrak{a}'$ ersetzt wird.

Nimmt man aber in (2) an Stelle des Ideals $\mathfrak{m}$ ein anderes Ideal $\mathfrak{m}_1$ und setzt

$$\mu_1 = \mathfrak{m}_1 \mathfrak{a}, \tag{4}$$

so ist

$$\frac{\mu}{\mu_1} = \frac{\mathfrak{m}}{\mathfrak{m}_1} = \eta$$

eine Zahl in $[O']$, also $\mathfrak{m}_1$ äquivalent mit $\mathfrak{m}$.

---

[1]) Unter einer Schar paralleler Formen versteht man das System

$$(a, b + 2la, c + lb + l^2 a),$$

wenn l alle ganzen rationalen Zahlen durchläuft.

Setzt man also

$$(5)\quad a_1 = N(\mathfrak{m}_1) = \mathfrak{m}_1 \mathfrak{m}_1', \quad \frac{b_1 + \sqrt{D}}{2} \equiv 0 \pmod{\mathfrak{m}_1},$$

so erhält man eine andere quadratische Form (a_1, b_1, c_1), von der wir nachweisen können, daß sie mit (a, b, c) äquivalent ist.

Wir setzen zur Abkürzung:

$$\omega = \frac{b + \sqrt{D}}{2a}, \quad \omega_1 = \frac{b_1 + \sqrt{D}}{2a_1}$$

und bemerken, daß

$$\eta a_1 = \eta \mathfrak{m}_1 \mathfrak{m}_1' = \mathfrak{m} \mathfrak{m}_1',$$
$$\eta \omega_1 a_1 = \frac{\mathfrak{m}}{\mathfrak{m}_1} \frac{b_1 + \sqrt{D}}{2}$$

durch $\mathfrak{m}$ teilbare Zahlen in $[Q]$ sind [nach (5)]. Demnach lassen sich nach § 97, 7. die ganzen rationalen Zahlen $\alpha, \beta, \gamma, \delta$ so bestimmen, daß:

$$(6)\quad \begin{aligned} \eta a_1 &= a(\alpha - \gamma \omega), \\ \eta a_1 \omega_1 &= a(-\beta + \delta \omega), \end{aligned}$$

und man beweist ganz wie in § 95, daß

$$\alpha\delta - \beta\gamma = 1$$

sein muß, daß also die beiden Formen

$$(a, b, c), \quad (a_1, b_1, c_1)$$

äquivalent sind. Wir haben also:

11. Satz. Jede durch ein Ideal $\mathfrak{a}$ repräsentierte Idealklasse nach $[Q]$ entspricht einer durch die Form (a, b, c) repräsentierten Formklasse A und umgekehrt.

Um die Formklasse A zu erhalten, nehme man ein primäres Ideal $\mathfrak{m}$ der zu A reziproken Klasse A^{-1} und setze $a = N(\mathfrak{m})$, $\frac{b + \sqrt{D}}{2} \equiv 0 \pmod{\mathfrak{m}}$. Und ist umgekehrt die Form (a, b, c) gegeben, so ist der größte gemeinschaftliche Teiler $\mathfrak{m}$ von

$$a, \quad \frac{b + \sqrt{D}}{2}$$

ein Ideal der Klasse A^{-1}.

§ 100. Idealklassen nach den Ordnungen.

Der Begriff der Äquivalenz der Ideale und die Sätze über Klassenzahlen lassen sich am übersichtlichsten darstellen, wenn

man die Ideale nach Bd. II, § 169 durch die in Bd. II, § 153 ff. besprochenen Funktionale repräsentiert, weil man dabei die gewöhnlichen Regeln der Multiplikation und Division benutzen kann[1]).

Wir beschränken uns hier ein für allemal in dem Körper Ω auf Zahlen und Ideale, die zu einer beliebig anzunehmenden ganzen rationalen Zahl Q (dem Führer einer Ordnung) teilerfremd sind.

Nach dieser Voraussetzung bilden die ganzen und gebrochenen Zahlen des Körpers Ω die vorher mit O bezeichnete Gruppe. Wir erweitern diese Gruppe durch Hinzufügung der Funktionale und bezeichnen die so erweiterte Gruppe mit $\overline{O}$. Jedem Element von $\overline{O}$ entspricht dann ein ganzes oder gebrochenes Ideal, und solchen Elementen, deren Quotient eine funktionale Einheit ist, entspricht dasselbe Ideal.

Ist η eine Zahl in O und ε irgend eine funktionale Einheit, so entspricht dem Produkt $\varepsilon\eta$ ein Hauptideal. Demnach bezeichnen wir

mit $\overline{E}$ die Gruppe der funktionalen Einheiten,
„ E „ „ „ numerischen Einheiten,

und durch

$\overline{E}O$ die Hauptklasse der Funktionale.

Nehmen wir ein Repräsentantensystem

(1) $$\varphi_1, \varphi_2, \ldots, \varphi_h$$

nicht äquivalenter ganzer Funktionale in Ω, so wird jedes ganze oder gebrochene Funktional Φ in der Weise darstellbar sein:

$$\Phi = \varphi_i \overline{\omega},$$

wo $\overline{\omega}$ ein Funktional aus $\overline{E}O$ ist, und die Idealklassen in Ω sind die Nebengruppen von $\overline{E}O$ in $\overline{O}$. Demnach ist die Klassenzahl h der Index des Teilers $\overline{E}O$ von $\overline{O}$:

(2) $$h = (\overline{O}, E O).$$

Hierbei hat man sich bei der schärferen Klasseneinteilung bei O auf die Zahlen mit positiver Norm zu beschränken.

Betrachten wir nun die Klasseneinteilung der Ideale nach der Ordnung $[Q]$, so haben wir als Hauptklasse die Funktionalgruppe $\overline{E}O'$ zu betrachten und die Klassenzahl ist

$$h' = (\overline{O}, \overline{E}O').$$

[1]) Vgl. auch des Verfassers Abhandlung „Über Zahlengruppen in algebraischen Körpern“, erste Mitteilung, Mathematische Annalen **48**, 438.

Um hieraus die Beziehung zwischen h und h' herzuleiten, machen wir von den allgemeinen Gruppensätzen Bd. II, § 2 Gebrauch, die wir folgendermaßen formulieren und ergänzen:

12. Satz. Ist A eine Gruppe und B ein Teiler von A von endlichem Index (A, B), ferner C ein Teiler von B von endlichem Index (B, C), so ist Bd. II, § 2, (4):

$$(A, C) = (A, B)\,(B, C). \tag{4}$$

Ist A wieder eine Gruppe mit dem Teiler B vom Index μ, so setzen wir

$$A = a_1 B + a_2 B + \cdots + a_\mu B, \tag{5}$$

worin $a_1, a_2, \ldots, a_\mu$ ein volles Repräsentantensystem von A nach B ist.

Es sei nun C eine Gruppe von Elementen, die mit den Elementen von A zusammensetzbar sind (z. B. in unserem Falle einfach durch Multiplikation), so ergibt sich aus (5):

$$A\,C = a_1 B\,C + a_2 B\,C + \cdots + a_\mu B\,C. \tag{6}$$

Nun kann in den beiden Nebengruppen $a_1 B\,C$, $a_2 B\,C$ nur dann ein und dasselbe Element vorkommen, wenn $a_1 a_2^{-1}$ in $B\,C$, aber nicht in B enthalten ist.

Daraus formulieren wir den Satz:

13. Satz. Ist A eine Gruppe, B ein Teiler von A vom endlichen Index (A, B), ferner C eine mit A zusammensetzbare Gruppe von der Art, daß A und $B\,C$ außer den B keine gemeinschaftlichen Elemente enthalten, so ist

$$(A\,C, B\,C) = (A, B). \tag{7}$$

Die Voraussetzung dieses Satzes läßt sich auch so aussprechen:

B ist der Durchschnitt von A und $B\,C$,

und sie ist z. B. erfüllt, wenn C in B enthalten, also $B = B\,C$ ist, und auch dann, wenn C mit A kein Element gemein hat.

14. Satz. Ist A eine aus den beiden Gruppen A' und B zusammengesetzte Gruppe

$$A = A'B \tag{8}$$

und B' der Durchschnitt von A' und B, so ist

$$(A, B) = (A', B'), \tag{9}$$

vorausgesetzt, daß diese Indices endlich sind.

Denn nach (8) ist in jeder Nebengruppe aB zu B in A ein Element a' aus A' enthalten, und man kann also diese Neben-

gruppen auch durch $a'B$ darstellen, wo a' in A' enthalten ist. Sind dann $a'_1 B$, $a'_2 B$ verschiedene Nebengruppen zu B in A, so sind $a'_1 B'$, $a'_2 B'$ verschiedene Nebengruppen zu B' in A' und umgekehrt; denn $a'_1 a'^{-1}_2$ ist dann und nur dann in B' enthalten, wenn es zugleich in B enthalten ist, und daraus folgt die Formel (9).

Diese Sätze wenden wir nun auf die Ausdrücke (2) und (3) für h und h' an. Nach (4) ist

$$(10) \qquad (\overline{O}, \overline{E}\,O') = (\overline{O}, \overline{E}\,O)\,(\overline{E}\,O, \overline{E}\,O'),$$

also

$$(11) \qquad h' = h\,(\overline{E}\,O, \overline{E}\,O').$$

Wir bezeichnen jetzt, wie schon oben, mit E die Gruppe der numerischen Einheiten in O. Dann ist $\overline{E}E = \overline{E}$, da die numerischen Einheiten unter den funktionalen enthalten sind, und jede Zahl, die in $\overline{E}\,O'$ enthalten ist, ist in $E\,O'$ enthalten. Folglich ist $E\,O'$ der Durchschnitt von O und $\overline{E}\,O'$. Wenden wir also (7) an, indem wir O, $E\,O'$, $\overline{E}$ an Stelle von A; B, C setzen, so ist B der Durchschnitt von A und BC und wir erhalten:

$$(12) \qquad (\overline{E}\,O, \overline{E}\,O') = (\overline{E}\,O, \overline{E}E\,O') = (O, E\,O').$$

Es ist ferner nach (4):

$$(13) \qquad (O, E\,O')\,(E\,O', O') = (O, O'),$$

und wenn wir mit E' die Gruppe der numerischen Einheit in O', also den Durchschnitt von E mit O' bezeichnen, so daß $E'\,O' = O'$ ist:

$$(E\,O', O') = (E\,O', E'\,O') = (E, E')$$

(nach 2), denn E' ist der Durchschnitt von $E'\,O'$ und E.

Also haben wir nach (13)

$$(O, E\,O')\,(E, E') = (O, O')$$

und nach (12)

$$(\overline{E}\,O, \overline{E}\,O')\,(EE') = (O, O'),$$

also schließlich nach (11):

$$(14) \qquad (E, E')\,h' = (O, O')\,h.$$

15. Satz. Die Formel (14) gilt unverändert, wenn O' nicht gerade die Ordnungsgruppe, sondern irgend eine in O enthaltene Zahlgruppe von endlichem Index (O, O') bedeutet, wenn wir zwei Ideale $\mathfrak{a}$, $\mathfrak{a}'$ nach O' äquivalent nennen, falls ihr Quotient $\mathfrak{a}'/\mathfrak{a} = \eta'$ eine Zahl in O' ist.

Ist E' die Gruppe der in O' enthaltenen Einheiten, und hat (E, E') einen endlichen Wert, so ist die Klassenzahl h' endlich und durch die Formel (12) bestimmt.

Ist z. B. O die Gruppe aller Zahlen in Ω (außer 0), O' die Gruppe der Zahlen mit positiver Norm, so ist, falls es überhaupt Zahlen mit negativer Norm gibt, $(O, O') = 2$. Gibt es dann Einheiten mit negativer Norm, so ist auch $(E, E') = 2$. Haben aber alle Einheiten positive Norm, so ist $(E, E') = 1$, und wir erhalten im ersten Falle $h' = h$, im zweiten Falle $2h' = h$.

Die Äquivalenz nach O ist dann die allgemeine Äquivalenz, die nach O' die verschärfte.

Kehren wir zu den Ordnungen $[Q]$ zurück und verstehen unter O die zu Q teilerfremden Zahlen (wenn nötig nur die mit positiver Norm), so haben wir (O, O') im vorigen Paragraphen bestimmt.

Ist die Diskriminante D und ihr Stamm Δ negativ, so gibt es im allgemeinen sowohl in E als in E' nur die zwei Einheiten ± 1. In den beiden Ausnahmefällen $\Delta = -3, -4$ enthält E sechs und vier Einheiten, E' aber, wenn $Q > 1$ ist, nur zwei, und es ist also $(E, E') = 1$ im allgemeinen, $(E, E') = 3$ im Falle $\Delta = -3$, $(E, E') = 2$ im Falle $\Delta = -4$. Also haben wir in diesen Fällen nach § 98, (10):

$$\lambda h' = Q \Pi \left(1 - \frac{(\Delta, q)}{q}\right) h, \tag{15}$$

worin:

$$\begin{array}{lll} \lambda = 2, & \text{für } \Delta = -4 \\ \lambda = 3, & \text{,, } \Delta = -3 \\ \lambda = 1, & \text{,, } \Delta < -4 \end{array} \tag{16}$$

Dies ist die Beziehung, die zuerst von Gauss abgeleitet und später von Dirichlet auf anderem Wege bestätigt ist.

Ist z. B. $\Delta \equiv 1 \pmod 4$, $Q = 2$, so ist nach Gaussscher Bezeichnung h die Klassenzahl für die Formen zweiter, h' die der Formen erster Art. Es ist

$$Q\left(1 - \frac{(\Delta, q)}{2}\right) = 1, \quad \Delta \equiv 1 \pmod 8,$$
$$= 3, \quad \Delta \equiv 5 \pmod 8.$$

Also

$$\begin{array}{ll} h' = h, & \Delta \equiv 1 \\ = 3h, & \Delta \equiv 5 \end{array} \pmod 8,$$

und nur in dem Ausnahmefalle $\Delta = -3$ kommt $h' = h$.

Ist D positiv, so ist noch (E, E') zu bestimmen.

Es sei

$$\varepsilon = \frac{t + u\sqrt{D}}{2}$$

die fundamentale Einheit in O und λ der kleinste positive Exponent, für den

$$\varepsilon^{\lambda} = \frac{t + u\sqrt{D}}{2}$$

in O' enthalten ist. Dann besteht E aus den Potenzen $\pm\varepsilon^{\nu}$, und E' aus den Potenzen $\pm\varepsilon^{\lambda\nu}$, und es ist

$$(E, E') = \lambda,$$

und die Formel (15) gibt die Klassenzahl h'. Eine weitere Bestimmung läßt sich im allgemeinen für λ nicht geben.

Ist wieder $\Delta \equiv 1 \pmod 4$ und $Q = 2$, so ist $\lambda = 1$ oder $= 3$; nämlich $= 1$, wenn in (17) u gerade ist, und $= 3$, wenn u ungerade ist. Letzteres kann nur vorkommen, wenn $\Delta \equiv 5 \pmod 8$ ist, und folglich ist für $\Delta \equiv 1 \pmod 8$ immer $\lambda = 1$, während für $\Delta \equiv 1 \pmod 8$ λ sowohl $= 1$ als $= 3$ sein kann.

Vierzehnter Abschnitt.

Komposition der Formen und Ideale.

---

§ 101. Komposition in den Ordnungen.

Es sei Δ die Körperdiskriminante und $D = Q^2 \Delta$ die Diskriminante der Ordnung $[Q]$.

Ist $T = (a, b, c)$ eine primitive quadratische Form der Diskriminanten D mit positivem, zu Q teilerfremdem a, so können wir daraus eine Basisform λ in O eines zu Q teilerfremden Ideals $\mathfrak{a}$ in folgender Weise bestimmen:

Wir setzen

(1) $$\lambda = a t_1 + \frac{b + \sqrt{D}}{2} t_2,$$

(2) $$N(\lambda) = a\,(a t_1^2 + b t_1 t_2 + c t_2^2).$$

Bezeichnen wir das durch das Funktional λ bestimmte Ideal, d. h. den größten gemeinschaftlichen Teiler von

(3) $$a, \frac{b + \sqrt{D}}{2}$$

mit $\mathfrak{a}$, so folgt aus (2)

(4) $$N(\mathfrak{a}) = a.$$

Hierin ist a die kleinste durch $\mathfrak{a}$ teilbare natürliche Zahl. Denn ist diese kleinste Zahl a_1, so muß a_1 ein Teiler von a sein, also etwa $a = a_1 a_2$. Hierin können a_1, a_2, b keinen gemeinsamen Teiler haben, denn sie können erstens nicht alle drei gerade sein, weil sonst $a = 4a'$, $b = 2b'$, $c = c'$,

$$D = 4(b'^2 - 4a'c)$$

wäre, und 4 müßte in Q aufgehen, entgegen der Annahme, daß a zu Q teilerfremd sei; und ebenso würde ein ungerader gemeinschaftlicher Primteiler von a_1, b, a_2 in Q aufgehen.

Setzen wir also

$$\lambda_1 = a_1 t_1 + \frac{b + \sqrt{D}}{2} t_2,$$

so wird

$$N(\lambda_1) = a_1 (a_1 t_1^2 + b t_1 t_2 + a_2 c t_2^2),$$

und $(a_1, b, a_2 c)$ ist gleichfalls primitiv. Da nun λ_1 durch $\mathfrak{a}$ teilbar ist, so muß a_1 durch $N(\mathfrak{a})$, d. h. durch a teilbar und mithin $= a$ sein. Also ist $\mathfrak{a}$ primär.

Wenn wir in (1) die $\sqrt{D}$ ein für allemal fest bestimmen, z. B. positiv reell oder positiv imaginär, so ist die lineare Form λ durch die quadratische Form T eindeutig bestimmt. Die Form des konjugierten Ideals würde nicht durch Änderung des Vorzeichens von $\sqrt{D}$, sondern von b erhalten.

Es seien $\mathfrak{a}$ und $\mathfrak{b}$ irgend zwei zum Führer Q der Ordnung $[Q]$, die wir jetzt mit O bezeichnen wollen, teilerfremde Ideale, und

$$(5) \qquad \begin{aligned} \mu &= \alpha_1 u_1 + \alpha_2 u_2, \\ \nu &= \beta_1 v_1 + \beta_2 v_2 \end{aligned}$$

seien Basisformen von $\mathfrak{a}$ und $\mathfrak{b}$ in O. Aus $\mathfrak{a}$ und $\mathfrak{b}$ bilden wir das Produkt

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}$$

mit der Basisform in O:

$$(6) \qquad \lambda = \gamma_1 t_1 + \gamma_2 t_2.$$

Die zu μ, ν, λ gehörigen quadratischen Formen mögen in U, V, T bezeichnet sein.

1. Wir nennen λ aus μ und ν, T aus U und V zusammengesetzt oder komponiert.

Wir setzen:

$$(7) \qquad \begin{aligned} T &= (a, b, c), \\ U &= (a_1, b_1, c_1), \\ V &= (a_2, b_2, c_2), \end{aligned}$$

und unsere Aufgabe ist gelöst, wenn T aus U und V abgeleitet werden kann.

Ist

$\mathfrak{a}$ äquivalent mit $\mathfrak{a}'$,
$\mathfrak{b}$ „ „ $\mathfrak{b}'$,

so ist auch

$\mathfrak{a}\mathfrak{b}$ „ „ $\mathfrak{a}'\mathfrak{b}'$,

also

$\mathfrak{c}$ „ „ $\mathfrak{c}'$,

und wenn also U, V durch äquivalente Formen U', V' ersetzt werden, so tritt auch an Stelle von T eine äquivalente Form T'.

Bezeichnen wir die Klassen in O, zu denen λ, μ, ν gehören, mit A, B, C und bezeichnen ebenso die Klassen der quadratischen Formen U, V, T, so heißt auch C aus A und B **komponiert**, und man setzt symbolisch

(8) $$C = AB.$$

Diese **Komposition der Klassen** ist eindeutig bestimmt, wenn irgend drei Repräsentanten U, V, T derselben gegeben sind, und es genügt also, wenn wir U, V in ihren Klassen irgendwie passend wählen.

In jeder Idealklasse gibt es Ideale, die zu einem beliebigen Ideal relativ prim sind. Wir nehmen also zunächst $\mathfrak{a}$ in A primär, sonst beliebig, dann $\mathfrak{b}$ gleichfalls primär und relativ prim, nicht nur zu $\mathfrak{a}$, sondern zu a_1. Dann sind a_1 und a_2 relativ prim (denn der größte gemeinschaftliche Teiler d von a_1 und a_2 wäre relativ prim zu $\mathfrak{b}$, und folglich wäre $a_2 : d$ durch $\mathfrak{b}$ teilbar). Daraus folgt aber $d = 1$, weil a_2 die kleinste durch $\mathfrak{b}$ teilbare natürliche Zahl sein sollte.

Hat man a_1, a_2 so bestimmt, so kann man b den beiden Kongruenzen

$$b \equiv b_1 \pmod{2a_1},$$
$$\equiv b_2 \pmod{2a_2}$$

gemäß bestimmen, und dann ist

$$b^2 - D = 4a_1 a_2 c$$

durch $4a_1 a_2$ teilbar. Wir setzen also

(9) $$U = (a_1, b, a_2 c),$$
$$V = (a_2, b, a_1 c).$$

Es ist $a_1 a_2$ die kleinste durch $\mathfrak{a}\mathfrak{b}$ teilbare ganze rationale Zahl, und $\mathfrak{a}\mathfrak{b}$ ist der größte gemeinschaftliche Teiler von

$$a_1 a_2, \quad \frac{b - \sqrt{D}}{2};$$

folglich ist

(10) $$T = (a_1 a_2, b, c)$$

die aus U und V komponierte Form, und die den quadratischen Formen T, U, V entsprechenden Linearformen λ, μ, ν sind:

$$\lambda = a_1 a_2 t_1 + \frac{b - \sqrt{D}}{2} t_2,$$

$$\mu = a_1 u_1 + \frac{b - \sqrt{D}}{2} u_2,$$

$$\nu = a_2 v_1 + \frac{b - \sqrt{D}}{2} v_2.$$

Daraus folgt, mit Rücksicht auf

$$\left(\frac{b-\sqrt{D}}{2}\right)^2 = a_1 a_2 c + b\,\frac{b-\sqrt{D}}{2}:$$

(11) $$\mu\nu = a_1 a_2 (u_1 v_1 - c u_2 v_2) + \frac{b-\sqrt{D}}{2}(a_1 u_1 v_2 + a_2 u_2 v_1 + b u_2 v_2).$$

Macht man also die bilineare Substitution:

(12) $$t_1 = u_1 v_1 - c u_2 v_2,$$
$$t_2 = a_1 u_1 v_2 + a_2 u_2 v_1 + b u_2 v_2,$$

so ergibt sich

(13) $$\lambda = \mu\nu,$$

und folglich

(14) $$T = UV.$$

In der Forderung, daß a_1 und a_2 relativ prim sein sollen, liegt bisweilen eine gewisse Unbequemlichkeit, z. B. wenn es sich um die Komposition einer Form mit sich selbst handelt.

Lassen wir also die Voraussetzung fallen, daß $\mathfrak{a}$ zu $\mathfrak{b}$ und a_1 zu a_2 relativ prim seien, halten dagegen an der Annahme fest, daß

(15) $$b^2 - D = 4 a_1 a_2 c$$

durch $4 a_1 a_2$ teilbar sei, so gilt die Relation (11) noch, und es folgt, daß $\mathfrak{a}\mathfrak{b}$ der größte gemeinschaftliche Teiler von

$$a_1 a_2,\quad a_1\frac{b-\sqrt{D}}{2},\quad a_2\frac{b-\sqrt{D}}{2},\quad b\,\frac{b-\sqrt{D}}{2}$$

ist (Bd. II, § 160, 2).

Haben nun a_1, a_2, b keinen gemeinschaftlichen Teiler, so kann man der Gleichung $k_1 a_1 + k_2 a_2 + k b = 1$ durch ganze rationale k genügen, und demnach ist $\mathfrak{a}\mathfrak{b}$ auch der größte gemeinschaftliche Teiler von

(16) $$a_1 a_2,\quad \frac{b-\sqrt{D}}{2}.$$

2. Es ist zu beweisen, daß $a_1 a_2$ die kleinste durch $\mathfrak{a}\mathfrak{b}$ teilbare natürliche Zahl ist.

Setzen wir nämlich diese kleinste Zahl $= a$, so ist $a_1 a_2$ durch a teilbar, etwa

$$a_1 a_2 = a a'.$$

Bilden wir die beiden Formen

$$\lambda = a_1 a_2 t_1 + \frac{b - \sqrt{D}}{2} t_2,$$

$$\lambda' = a t_1 + \frac{b - \sqrt{D}}{2} t_2,$$

so folgt:

$$N(\lambda) = a_1 a_2 (a_1 a_2 t_1^2 + b t_1 t_2 + c t_2^2),$$
$$N(\lambda') = a (a t_1^2 + b t_1 t_2 + a' c t_2^2).$$

Die beiden Formen $(a_1 a_2, b, c)$, $(a, b, a' c)$ sind primitiv (weil ein gemeinsamer Primteiler von $a_1 a_2$, b, c wegen (15) in Q aufgehen müßte), und es folgt für die absolute Norm:

$$N_a(\lambda) = a_1 a_2 = N(\mathfrak{a}\mathfrak{b}),$$
$$N_a(\lambda') = a;$$

da aber λ' durch $\mathfrak{a}\mathfrak{b}$ teilbar ist, so muß a durch $a_1 a_2$ teilbar und mithin $a' = 1$ sein.

Hieraus ergibt sich:

3. Sind a_1, a_2, b ohne gemeinsamen Teiler und

$$D = b^2 - 4 a_1 a_2 c,$$

so ist die Form

$$T = (a_1 a_2, b, c)$$

aus den beiden Formen

$$U = (a_1, b, c a_2), \quad V = (a_2, b, c a_1)$$

komponiert.

Wendet man dies auf zwei entgegengesetzte Formen

$$U = (a, b, c), \quad V = (c, b, a)$$

an, so ergibt sich

$$T = (a c, b, 1),$$

und dies ist mit der Hauptform $\left(1, 0, \frac{-D}{4}\right)$ oder $\left(1, 1, \frac{1-D}{4}\right)$ äquivalent.

4. Zwei entgegengesetzte Klassen geben komponiert die Hauptklasse.

Um eine Klasse A wiederholt mit sich selbst zusammenzusetzen, wähle man $\mathfrak{a}$ in A so, daß es relativ prim zu D ist, und bezeichne mit (a, b, c) die entsprechende Form. Dann ist a relativ prim zu b. Denn wäre d ein Teiler von a und b, so wäre d auch in D enthalten, also relativ prim zu $\mathfrak{a}$. Es wäre also auch $a:d$ durch a teilbar, was, wenn $d > 1$ ist, der Definition von a widerspricht.

Nun kann man aber b so wählen, daß

(17) $$b^2 \equiv D \pmod{4\, a^n}$$

ist, für ein beliebig großes n. Denn man kann b um ein beliebiges Vielfaches von $2\, a$ verändern. Nehmen wir also (17) als erfüllt an für einen Exponenten n, und setzen demgemäß

(18) $$b^2 = D + 4\, a^n\, c,$$

so folgt:

$$(b + 2\, h\, a^n)^2 - D \equiv 4\, a^n\, (c + h\, b) \pmod{4\, a^{n+1}},$$

und wenn man also h aus der Kongruenz $c + h\, b \equiv 0 \pmod{a}$ bestimmt, so ergibt sich ein der Kongruenz (17) für $n + 1$ genügendes b.

Da nun b relativ prim zu a ist, so folgt nach 2., daß, wenn $n \geqq m$ ist, a^m die kleinste durch $\mathfrak{a}^m$ teilbare natürliche Zahl ist, und daraus ergibt sich folgende Kompositionsregel:

5. Genügt die Form $(a, b, a^n c) = U$ der Bedingung (18), und ist $m \leqq n$, so ist

$$U^m = (a^m, b, a^{n-m}\, c).$$

Hiermit sind die Klassen quadratischer Formen der Diskriminante Δ zu einer Abelschen Gruppe vereinigt, die mit der Gruppe der Idealklassen isomorph ist, und es ist zugleich ein Weg angegeben, wie man durch passend gewählte Repräsentanten die Komposition in diesen Gruppen wirklich ausführen kann [1]).

§ 102. Komposition der Ordnungen.

Eine Ordnung $O = [Q]$ im Körper Ω ist durch den Führer Q vollständig bestimmt. Es seien O_1, O_2 zwei Ordnungen mit den Führern Q_1, Q_2, und der größte gemeinschaftliche Teiler von Q_1 und Q_2 sei Q. Ist dann M das kleinste gemeinschaftliche Multiplum von Q_1 und Q_2, so ist

(1) $$Q_1\, Q_2 = Q\, M.$$

---

[1]) Die Einheit in der Gruppe der Klassen bildet die Hauptklasse. Über die Komposition der quadratischen Formen ist zu erwähnen: Gauss, „Disquisitiones arithmeticae“, Art. 235 u. f. Dirichlet, De formarum binariarum secundi gradus compositione (1851), Werke Bd. II, S. 105. Dirichlet-Dedekind, Vorlesungen über Zahlentheorie, 4. Aufl., § 145 f. Dedekind, Crelles Journal, Bd. 129. H. Weber, Göttinger Nachrichten, 9. Februar 1907.

6. Die zum Führer Q gehörige Ordnung O heißt aus O_1 und O_2 zusammengesetzt oder komponiert.

Wir setzen symbolisch

(2) $$O = O_1 O_2.$$

Die Diskriminanten dieser drei Ordnungen sind

(3) $$D = Q^2 \Delta, \quad D_1 = Q_1^2 \Delta, \quad D_2 = Q_2^2 \Delta.$$

Sind Q_1 und Q_2 relativ prim, so ist die aus beiden komponierte Ordnung die Hauptordnung O_0.

Um die Komposition der Ordnungen auszuführen, kann man ebenso verfahren, wie im vorigen Paragraphen. Wir setzen

(4) $$Q_1 = Q m_1, \quad Q_2 = Q m_2,$$

und dann sind m_1, m_2 relativ prim zueinander.

Es mögen dann $\mathfrak{a}$ und $\mathfrak{b}$ zwei Ideale bedeuten, die zu $Q_1 Q_2$ relativ prim sind.

Ist dann

$$\begin{aligned} &\mathfrak{a} \text{ äquivalent } \mathfrak{a}' \text{ nach } O_1, \\ &\mathfrak{b} \quad\ \text{"} \qquad \mathfrak{b}' \ \text{"} \ \ O_2, \end{aligned}$$

so ist

$$\begin{aligned} \frac{\mathfrak{a}}{\mathfrak{a}'} &= \eta_1 \text{ eine Zahl in } O_1, \\ \frac{\mathfrak{b}}{\mathfrak{b}'} &= \eta_2 \quad \text{"} \quad \text{"} \quad \text{"} \ \ O_2, \end{aligned}$$

d. h. η_1 ist nach dem Modul Q_1, η_2 nach dem Modul Q_2 mit einer rationalen Zahl kongruent. Also sind beide, und folglich ihr Produkt, nach dem Modul Q mit einer rationalen Zahl kongruent und gehören in die Ordnung Q. Demnach ist auch

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b} \text{ äquivalent mit } \mathfrak{c}' = \mathfrak{a}'\mathfrak{b}' \text{ nach } O.$$

Es sei a_1 die kleinste durch $\mathfrak{a}$ teilbare natürliche Zahl und $\mathfrak{b}$ relativ prim zu a_1 (folglich auch zu $\mathfrak{a}$), und wenn a_2 die kleinste durch $\mathfrak{b}$ teilbare natürliche Zahl ist, so sind auch a_1 und a_2 relativ prim. Man kann dann immer, was auch b_1, b_2 sein mögen, den Kongruenzen

$$\begin{aligned} b_1 &\equiv m_1 b \pmod{2 a_1}, \\ b_2 &\equiv m_2 b \pmod{2 a_2} \end{aligned}$$

genügen und demnach die Basisformen von $\mathfrak{a}$ und $\mathfrak{b}$ in der Gestalt annehmen:

$$\mu = a_1 u_1 + m_1 \frac{b - \sqrt{D}}{2} u_2,$$

$$\nu = a_2 v_1 + m_2 \frac{b - \sqrt{D}}{2} v_2,$$

und es ist

$$b^2 - D = 4 a_1 a_2 c$$

durch $4 a_1 a_2$ teilbar. Dann ist $a_1 a_2$ die kleinste durch $\mathfrak{a}\mathfrak{b}$ teilbare natürliche Zahl, und es ist

$$\lambda = a_1 a_2 t_1 + \frac{b - \sqrt{D}}{2} t_2$$

eine Basisform von $\mathfrak{c}$.

Demnach gibt die Zusammensetzung der entsprechenden quadratischen Formen der Diskriminanten D_1, D_2:

(5)
$$U = (a_1, m_1 b, m_1^2 a_2 c),$$
$$V = (a_2, m_2 b, m_2^2 a_1 c),$$

die Form T der Diskriminante D:

(6)
$$T = (a_1 a_2, b, c).$$

Fünfzehnter Abschnitt.

Geschlechter der quadratischen Formen.

§ 103. Darstellung von Zahlen durch quadratische Formen.

Eine natürliche Zahl m heißt durch die primitive Form (a, b, c) mit der Diskriminante D eigentlich darstellbar, wenn es zwei relative Primzahlen x, y gibt, die die Gleichung

(1) $$ax^2 + bxy + cy^2 = m$$

erfüllen, und man kann eine mit (a, b, c) äquivalente Form (m, n, l) finden, deren Diskriminante

(2) $$D = n^2 - 4ml$$

ist. Ist m durch die Form (a, b, c) darstellbar, so ist sie auch durch jede äquivalente Form, also durch jede Form der Klasse A, zu der (a, b, c) gehört, darstellbar. Wir nennen dann m durch die Klasse A darstellbar. Sind A, A' zwei Klassen, m, m' zwei zueinander teilerfremde Zahlen, die durch diese Klasse eigentlich darstellbar sind, so ist das Produkt mm' durch die zusammengesetzte Klasse AA' eigentlich darstellbar. Dies folgt aus den Kompositionen der Formen (12), (14), § 101.

Aus (2) ergab sich:

(3) $$n^2 \equiv D \pmod{4m}.$$

Ist (m, n, l) imprimitiv, so kann D keine Stammdiskriminante sein. Wir bezeichnen, wie bisher, den Stamm von D mit Δ und setzen

$$D = Q^2 \Delta,$$

und der größte gemeinschaftliche Teiler von m, n, l geht in Q^2 auf. Wir nehmen daher im Folgenden an, m sei relativ prim zu Q, und sind dann sicher, daß die durch (2) bestimmte Form (m, n, l) primitiv ist.

Ist umgekehrt die Kongruenz (3) erfüllt, so kann man $D = n^2 - 4ml$ setzen und erhält eine Form der Diskriminante D, (m, n, l), durch die m eigentlich darstellbar ist.

1. Die notwendige und hinreichende Bedingung dafür, daß eine zu Q teilerfremde Zahl m durch eine Form der Diskriminante D eigentlich darstellbar ist, besteht also darin, daß die Kongruenz

(4) $$x^2 \equiv D \pmod{4m}$$

lösbar sei.

Aus einer Form (a, b, c) erhält man eine Schar äquivalenter Formen:

(5) $$(a,\ b + 2\lambda a,\ C),$$

worin λ eine beliebige ganze Zahl und C durch die Gleichung

$$D = (b + 2\lambda a)^2 - 4aC$$

bestimmt ist und sich gleich $a\lambda^2 + b\lambda + c$ ergibt. Das System (5) wird eine Schar paralleler Formen genannt.

Wenn die Kongruenz (4) erfüllt ist, so ist auch

$$(x + 2\lambda m)^2 \equiv D \pmod{4m},$$

und wir wollen die ganze Schar der Wurzeln von (4), die nach dem Modul $2m$ kongruent sind, als eine Wurzel betrachten. In diesem Sinne sei die Anzahl der Wurzeln von (4), die demnach sicher endlich ist, mit $\psi(D, m)$ zu bezeichnen.

2. Jede Wurzel von (4) gibt Anlaß zu einer Schar paralleler Formen, durch die die Zahl m eigentlich darstellbar ist.

Die Zahl $\psi(D, m)$ läßt sich leicht bestimmen. Sind zunächst m', m'' relativ prim, so ist

(6) $$\psi(D, m'), \psi(D, m'') = \psi(D, m'm'').$$

Denn ist

(7) $$x'^2 \equiv D \pmod{4m'}, \quad x''^2 \equiv D \pmod{4m''},$$

und

(8) $$\begin{aligned} x &\equiv x' \pmod{2m'}, \\ &\equiv x'' \pmod{2m''}, \end{aligned}$$

so ist $(x^2 - D) : 4$ durch m' und durch m'', also auch durch $m'm''$ teilbar, und die Kongruenz

(9) $$x^2 \equiv D \pmod{4m'm''}$$

erfüllt. Umgekehrt gibt jede Wurzel der Kongruenz (9) je eine Wurzel der beiden Kongruenzen (7). Also erhält man alle

Wurzeln von (9) und nur diese, wenn man in (8) die Wurzeln x', x'' von (7) paarweise kombiniert, und daraus folgt (6).

Nach (6) ist nur noch nötig, die Funktion $\psi(D, m)$ für den Fall zu bestimmen, daß $m = q^k$ eine Potenz einer in Q nicht aufgehenden Primzahl q ist. Wir brauchen das Symbol (D, n) in dem in § 85 erklärten Sinn und unterscheiden drei Fälle:

1) Wenn q in Δ aufgeht, so ist $(D, q) = 0$, und die Kongruenz (3) hat nur dann eine Lösung, wenn $k = 1$ ist, nämlich je nachdem D gerade oder ungerade, ist $x \equiv 0$ oder $\equiv q \pmod{2q}$, dagegen keine Lösung, wenn $k > 1$ ist, und dies gilt auch für $q = 2$. Denn in diesem Falle müßte Q ungerade, Δ durch 4 teilbar sein, folglich x gerade. Die Kongruenz

$$\left(\frac{x}{2}\right)^2 \equiv Q^2 \frac{\Delta}{4} \pmod{2^k}$$

ist aber nur lösbar für $k = 1$, da $\Delta : 4$ keine Diskriminante ist.

2) Ist $(D, q) = -1$, so ist die Kongruenz (3) nicht lösbar, weil dann D quadratischer Nichtrest von q oder (für $q = 2$) von 8 ist.

3) Ist $(D, q) = +1$, so ist D quadratischer Rest von q (oder von 8) und die Kongruenz,

$$x^2 \equiv D \mod 4q^k$$

hat, wie aus der Zahlentheorie bekannt ist, zwei Wurzeln.

Wir fassen diese Resultate übersichtlich so zusammen:

$$\begin{array}{lll} \text{Ist 1) } (D,q) = 0, & \text{so ist } \psi(D,q) = 1, & \psi(D,q^k) = 0 \ (k > 1), \\ \text{„ 2) } (D,q) = -1, & \text{„ „ } \psi(D,q^k) = 0 & \multirow{2}{*}{$\Big\}\ (k \gtreqless 1),$} \\ \text{„ 3) } (D,q) = +1, & \text{„ „ } \psi(D,q^k) = 2 & \end{array}$$

wozu noch kommt:

$$\psi(D, 1) = 1.$$

Nach (5) ist also $\psi(D, m)$ immer dann gleich Null, wenn in m eine Primzahl aufgeht, für die $(D, q) = -1$ ist, oder wenn in m ein Primfaktor von D mehr als einmal aufgeht.

In den anderen Fällen ist $\psi(D, q)$ eine Potenz von 2, deren Exponent gleich der Anzahl der in m, aber nicht in D aufgehenden Primzahlen ist.

Zwischen den Symbolen $\psi(D, m)$ und (D, m) besteht die folgende allgemeine Beziehung immer unter der Voraussetzung, daß m relativ prim zu Q ist:

Es durchlaufe ε die sämtlichen Teiler von m (1 und m eingeschlossen) und e^2 die sämtlichen quadratischen Teiler von m; dann ist

$$(10) \qquad \sum^{e^2} \psi\left(D, \frac{m}{e^2}\right) = \sum^{\varepsilon} (D, \varepsilon).$$

Ist diese Relation richtig für zwei Zahlen m', m'', die keinen gemeinsamen Teiler haben, so folgt sie für $m = m'm''$. Denn haben e', ε' und e'', ε'' dieselbe Bedeutung für m' und m'', wie e, ε für m, so sind $\varepsilon = \varepsilon' \varepsilon''$ die Teiler und $e^2 = e'^2 e''^2$ die quadratischen Teiler von $m = m'm''$. Es ist aber nach (6) und § 85, (8):

$$\sum^{e'^2} \sum^{e''^2} \psi\left(D, \frac{m'}{e'^2}\right) \psi\left(D, \frac{m''}{e''^2}\right) = \sum^{e^2} \psi\left(D, \frac{m}{e^2}\right),$$

$$\sum^{\varepsilon'} \sum^{\varepsilon''} (D, \varepsilon')\,(D, \varepsilon'') = \Sigma (D, \varepsilon).$$

Hiernach brauchen wir die Relation (10) nur noch unter der Voraussetzung zu beweisen, daß $m = q^k$ eine Primzahlpotenz ist. Unter dieser Voraussetzung ist aber:

$$\frac{n}{e^2} = q^{k-2s}, \qquad 0 \leqq s \mathrel{\substack{=\\<}} \frac{k}{2},$$
$$\varepsilon = q^s, \qquad s = 0, 1, 2, \ldots, k.$$

Ist nun

1. $(D, q) = 0$, so ist $\sum^{s} \psi(D, q^{k-2s}) = 1$,
2. $(D, q) = -1$, „ „ $\sum^{s} \psi(D, q^{k-2s}) = 1$ (k gerade), $= 0$ (k ungerade),
3. $(D, q) = 1$, „ „ $\sum^{s} \psi(D, q^{k-2s}) = k + 1$,

und ebenso groß ergibt sich in den drei Fällen die Summe

$$\sum_{0,k}^{s} (D, q^s);$$

denn im Falle 1. hat nur das dem $s = 0$ entsprechende Glied dieser Summe den Wert 1, die anderen verschwinden; im Falle 2. haben die den geraden s entsprechenden Glieder den Wert $+1$, die anderen den Wert -1, und im Falle 3. haben alle $k+1$-Glieder den Wert $+1$.

Damit ist also die Relation (10) allgemein bewiesen.

§ 104. Charaktere und Geschlechter der quadratischen Formen.

Unter einem Stammteiler δ einer Diskriminante D wollen wir folgendes verstehen (§ 84):

1. δ ist eine in D aufgehende Stammdiskriminante.
2. Der Quotient $D : \delta = D_1$ ist selbst noch Diskriminante.

Ein ungerader Stammteiler kann keine anderen Primfaktoren enthalten als solche, die in D aufgehen, und keinen mehr als einmal; dagegen ist ein beliebiges Produkt aus verschiedenen in D aufgehenden ungeraden Primzahlen, mit einem solchen Vorzeichen versehen, daß $\delta \equiv 1 \pmod 4$ wird, immer ein Stammteiler.

Außerdem kommt noch unter den Stammteilern vor:

$$(1)\qquad \begin{array}{lll} -4, & \text{wenn} & D \equiv 0, -4 \pmod{16}, \\ +8, & \text{„} & D \equiv 0, \quad 8 \pmod{32}, \\ -8, & \text{„} & D \equiv 0, -8 \pmod{32}, \end{array}$$

Bezeichnen wir also mit δ_1 die ungeraden Stammteiler, so ergeben sich die sämtlichen Stammteiler δ:

$$\begin{array}{llll} 1) & \delta = \delta_1, & D \equiv & 1 \pmod{4}, \\ & & \equiv & 4 \pmod{16}, \\ 2) & \delta = \delta_1, \ -4\delta_1, & D \equiv & -4 \pmod{16}, \\ & & \equiv & 16 \pmod{32}, \\ 3) & \delta = \delta_1, \quad 8\delta_1, & D \equiv & 8 \pmod{32}, \\ 4) & \delta = \delta_1, \ -8\delta_1, & D \equiv & -8 \pmod{32}, \\ 5) & \delta = \delta_1, \ -4\delta_1, & D \equiv & 0 \pmod{32}. \\ & \quad 8\delta_1, \ -8\delta_1, & & \end{array}$$

Die Anzahl der Stammteiler (1 als Stammteiler mitgerechnet) ist hiernach stets eine Potenz von 2.

3. Setzen wir sie gleich 2^λ, so ist λ in den Fällen 1), 2), 3), 4) gleich der Anzahl der in D aufgehenden verschiedenen Primzahlen, in dem Falle 5) um eins größer.

Die Stammteiler von D lassen sich durch Anwendung einer symbolischen Multiplikation zu einer Abelschen Gruppe machen.

Wenn nämlich δ_1, δ_2 zwei Stammteiler von D sind, so ist das Produkt $\delta_1 \delta_2$ auch eine Diskriminante, aber nicht immer eine Stammdiskriminante. Wir bezeichnen mit δ den Stamm von $\delta_1 \delta_2$ und setzen symbolisch

$$(2)\qquad \delta = \delta_1 \delta_2.$$

Haben δ_1, δ_2 keinen gemeinschaftlichen Teiler, so ist diese symbolische Multiplikation eine wirkliche. Haben sie aber einen gemeinschaftlichen Teiler, so ist noch ein quadratischer Faktor aus dem wahren Produkt $\delta_1 \delta_2$ abzuwerfen. Setzen wir in (2) $\delta_1 = \delta_2$, so ist $\delta = 1$, d. h. es ist jedes Element der Gruppe der δ sich selbst reziprok, und es besteht zugleich mit (2):

$$\delta_1 = \delta \delta_2. \tag{3}$$

Die Elemente dieser Gruppe lassen sich folgendermaßen durch eine **Basis** darstellen (Bd. II, § 11):

$$\delta = \delta_1^{\varepsilon_1} \delta_2^{\varepsilon_2} \dots \delta_\lambda^{\varepsilon_\lambda}, \tag{4}$$

worin $\varepsilon_1, \varepsilon_2, \dots \varepsilon_\lambda$ die Werte 0 oder 1 haben, und λ die oben angegebene Bedeutung hat. $\delta_1, \delta_2, \dots \delta_\lambda$ sind in dem Falle 1) die in D aufgehenden ungeraden Primdiskriminanten $\pm p$, im Falle 2) kommt dazu noch -4, im Falle 3) 8, im Falle 4) -8, im Falle 5) 8 und -8 (oder -4 und 8 oder -4 und -8).

Mit Hilfe der Stammteiler werden nun die **Charaktere** der primitiven quadratischen Formen definiert.

Wir wählen in einer Formenklasse A einen Repräsentanten (a, b, c), in dem a positiv und relativ prim zu D ist. Ist dann eine zu D teilerfremde Zahl m durch A darstellbar, so ist

$$m = ax^2 + bxy + cy^2,$$
$$4am = (2ax + by)^2 - Dy^2. \tag{5}$$

Es sei nun δ ein Stammteiler von D und m **relativ prim** zu δ, so ist, zunächst für ein ungerades δ, nach § 85, (14), (16):

$$(\delta, m) = (\delta, a). \tag{6}$$

Diese Relation gilt aber auch für $\delta = -4\delta_1, +8\delta_1, -8\delta_1$. Denn es ist in diesen Fällen a und m ungerade und nach (1) und (5):

$$\begin{aligned}
\delta &= -4\delta_1, & D &\equiv 0, -4 \pmod{16}, & am &\equiv 1 \pmod 4,\\
\delta &= 8\delta_1, & D &\equiv 0, \ 8 \pmod{32}, & am &\equiv \pm 1 \pmod 8,\\
\delta &= -8\delta_1, & D &\equiv 0, -8 \pmod{32}, & am &\equiv 1, 3 \pmod 8,
\end{aligned}$$

woraus nach § 85 auch für diese Fälle die Gleichung (6) folgt, die danach allgemein bewiesen ist.

4. **Der Wert des Symbols (δ, m) ist also nicht von der Zahl m, sondern nur von der Formenklasse A abhängig, durch die m darstellbar ist. Es wird der zum Stammteiler δ gehörige Charakter dieser Klasse genannt und mit $\chi(\delta, A)$ bezeichnet.**

Es gilt zunächst für jede beliebige Klasse A und für beliebige Stammteiler δ, δ_1, δ_2:

(7) $$\chi(1, A) = 1,$$

(8) $$\chi(\delta_1, A)\, \chi(\delta_2, A) = \chi(\delta_1 \delta_2, A),$$

(9) $$\chi(\delta, A_0) = 1,$$

worin $\delta_1 \delta_2$ das oben definierte symbolische Produkt ist und A_0 die Hauptklasse bedeutet, durch die die Zahl 1 darstellbar ist.

Sind für eine Klasse A die Charaktere $\chi(\delta_1, A)$, $\chi(\delta_2, A) \ldots \chi(\delta_\lambda, A)$ gegeben, so sind nach (4) und (8) alle $\chi(\delta, A)$ bestimmt. Jeder dieser Charaktere kann aber $= +1$ oder $= -1$ sein, und so ergeben sich 2^λ mögliche Bestimmungen über die Charaktere. Diese sind aber nicht voneinander unabhängig.

Denn es folgt aus (5)

$$Dy^2 \equiv (2ax + by)^2 \pmod{4m},$$

und daraus folgt, wenn man m relativ prim zu a, folglich zu y annimmt:

$$(Dy^2, m) = (\Delta, m) = 1.$$

Daraus ergibt sich, daß für jede Klasse A

(10) $$\chi(\Delta, A) = +1.$$

Nun läßt sich zu jedem Stammteiler δ ein bestimmter, von δ verschiedener **komplementärer** Stammteiler δ' so bestimmen, daß im Sinne der symbolischen Multiplikation

(11) $$\delta\delta' = \Delta$$

ist. Das Komplement von δ' ist wieder δ, und jeder Primteiler, der in δ und δ' zugleich aufgeht, muß in Q aufgehen.

Daraus folgt nach (10) für jede Klasse A:

(12) $$\chi(\delta, A) = \chi(\delta', A),$$

und hiernach ist die Anzahl der möglichen Bestimmungen über die $\chi(\delta, A)$ nur noch $2^{\lambda-1}$.

Man vereinigt in ein **Geschlecht (Genus)** alle Formenklassen A, in denen sämtliche Charaktere $\chi(\delta, A)$ übereinstimmen, und gelangt zu dem Resultate:

5. **Die Anzahl der existierenden Geschlechter ist höchstens gleich $2^{\lambda-1}$.**

Ob die Anzahl der existierenden Geschlechter wirklich so groß ist, ist eine tiefere Frage, auf die wir später zurückkommen.

Wenn die Klasse A aus der Klasse A', A'' komponiert ist, so ist symbolisch

$$A = A' A''.$$

Sei m', m'' durch die Klasse A', A'' darstellbar, und nehmen wir m', m'' relativ prim, so ist $m = m'm''$ durch A darstellbar (§ 103), und daraus ergibt sich für die Charaktere die Formel:

$$\chi(\delta, A'A'') = \chi(\delta, A')\,\chi(\delta, A''). \tag{13}$$

Nach 1. ist das Symbol $\chi(\delta, A)$ durch irgend eine zu δ teilerfremde, durch A eigentlich darstellbare Zahl m bestimmt, und wir definieren daher die Charaktere dieser Zahlen m durch

$$\chi(\delta, m) = \chi(\delta, A). \tag{14}$$

Es ist aber zweckmäßig, daß man sich noch von der Voraussetzung frei macht, daß m zu δ relativ prim sei, und dies kann auf folgende Weise geschehen. An der Voraussetzung, daß m relativ prim zu Q sei, soll aber festgehalten werden.

Ist m durch die Klasse A eigentlich darstellbar, so können wir in A einen Repräsentanten

$$\varphi = (m, B, C) \tag{15}$$

finden. Wir zerlegen m in zwei Faktoren

$$m = nn', \tag{16}$$

so daß n und n' teilerfremd sind und n relativ prim zu δ, n' relativ prim zu δ' ist.

Dies ist immer möglich, meist auf mehrere Arten, da nach Voraussetzung m relativ prim zu Q ist, und also m, δ, δ' keinen gemeinschaftlichen Teiler haben. Man nehme z. B. in n die in δ' aufgehenden Primzahlen in so hohen Potenzen auf, als sie in m enthalten sind, und außerdem noch die Primzahlpotenzen, die zu δ teilerfremd sind.

Dann ist die Form φ aus den beiden Formen

$$(n, B, Cn') \qquad (n', B, Cn)$$

komponiert, deren Charaktere nach (12) und 4. durch

$$(\delta, n), \quad (\delta' n')$$

bestimmt sind, und es ist also nach (13):

$$\chi(\delta, A) = (\delta, n)(\delta', n'). \tag{17}$$

Hierin kann aber auch noch die Forderung aufgegeben werden, daß m durch A eigentlich darstellbar sei; denn ein gemeinsamer Teiler von x, y (relativ prim zu Q) gibt einen

quadratischen Teiler von m, den man wieder in zwei teilerfremde quadratische Faktoren zerlegt, von denen der eine zu n, der andere zu n' genommen wird, und dadurch ändern sich (δ, n) und (δ', n') nicht.

Man kann hiernach einen Charakter $\chi(\delta, n)$ einer beliebigen zu Q teilerfremden Zahl folgendermaßen bestimmen.

Man setze:

$$n = \varepsilon n' \tag{18}$$

und verstehe unter ε das Produkt der in n aufgehenden Potenzen solcher Primzahlen, die zugleich in δ aufgehen; dann ist ε relativ prim zu δ' und n' relativ prim zu δ, und man setze:

$$\chi(\delta, n) = (\delta', \varepsilon)(\delta, n'), \tag{19}$$

wodurch $\chi(\delta, n)$ eindeutig und immer von Null verschieden bestimmt ist. Ist dann (a, b, c) ein Repräsentant der Klasse A, so ist

$$\chi(\delta, ax^2 + bxy + cy^2) = \chi(\delta, A), \tag{20}$$

worin x, y beliebige ganze Zahlen mit oder ohne gemeinsamen Teiler sind, für die $ax^2 + bxy + cy^2$ teilerfremd zu Q wird.

Über das so definierte Symbol $\chi(\delta, n)$ gilt eine Reihe von Sätzen, die wir noch ableiten müssen.

6. Sind n_1 und n_2 irgend zwei zu Q teilerfremde Zahlen, so ist

$$\chi(\delta, n_1)\chi(\delta, n_2) = \chi(\delta, n_1 n_2). \tag{21}$$

Denn setzen wir nach (18)

$$n_1 = \varepsilon_1 n_1', \quad n_2 = \varepsilon_2 n_2',$$

so ist

$$n_1 n_2 = \varepsilon_1 \varepsilon_2 n_1' n_2',$$

und dies geht in (18) über, wenn man $n = n_1 n_2$, $\varepsilon = \varepsilon_1 \varepsilon_2$, $n' = n_1' n_2'$ setzt. Also folgt (21) aus § 103 (8).

7. Läßt man e die Reihe der Divisoren von n durchlaufen, und setzt $n = ee'$, so ist

$$\chi(\delta, n) \sum^{e} (D, e) = \sum^{e} (\delta, e)(\delta', e'). \tag{22}$$

Wenn die Formel (22) für $n = n_1$ und $n = n_2$ gilt, so gilt sie, unter der Voraussetzung, daß n_1, n_2 relativ prim sind, auch für $n = n_1 n_2$ [nach (21)]; sie braucht also nur noch für eine Primzahlpotenz $n = p^k$ bewiesen zu werden, wenn p nicht in Q

aufgeht. In diesem Falle ist aber $(D, p^s) = (\varDelta, p^s)$ [§ 85 (9)], und es ist also zu beweisen:

$$\chi(\delta, p^k) \sum_{0,k}^{s} (\varDelta, p^s) = \sum_{0,k}^{s} (\delta, p^s)(\delta', p^{k-s}).$$

Geht nun p nicht in δ auf, so ist

$$\chi(\delta, p^k) = (\delta, p^k),$$

und wenn man rechts jedes Glied unter dem Summenzeichen mit $(\delta, p^{k-s})^2 = 1$ multipliziert, so erhält man übereinstimmend mit der linken Seite

$$(\delta, p^k) \sum^{s} (\varDelta, p^{k-s}).$$

Geht aber p in δ und folglich nicht in δ' auf, so ist $\chi(\delta, p^k) = (\delta', p^k)$, multipliziert man also ebenso mit $(\delta', p^s)^2$, so folgt das gleiche, wodurch (22) bewiesen ist.

8. Ist $\chi(\delta, n)$ von $\chi(\delta', n)$ verschieden, so ist

(23) $$\Sigma(D, \bar{e}) = 0, \quad \Sigma(\delta, e)(\delta', e') = 0.$$

Denn da sich die beiden Summen nicht ändern, wenn δ mit δ' vertauscht wird, so folgt dies aus (22).

9. Sind δ_1, δ_2 zwei Stammteiler von D und $\delta_1\delta_2$ ihr symbolisches Produkt, so ist

(24) $$\chi(\delta_1, n)\,\chi(\delta_2, n) = \chi(\delta_1\delta_2, n).$$

Diese Formel braucht wegen (21) nur für den Fall bewiesen zu werden, daß n eine Primzahl ist.

Es ist aber symbolisch

$$(\delta_1\delta_2)' = \delta_1'\delta_2 = \delta_1\delta_2',$$

und hiernach ergibt sich (24) leicht aus der Definition (19).

§ 105. Anwendung des Legendreschen Symbols.

Will man sich der bekannteren Bezeichnung nach Legendre und Jacobi bedienen, so gestaltet sich die Sache folgendermaßen.

Bedeutet l eine ungerade Primzahl und a eine durch l nicht teilbare Zahl, so ist nach Legendre:

(1) $$\left(\frac{a}{l}\right) = +1,$$

wenn a quadratischer Rest von l ist,

$$\left(\frac{a}{l}\right) = -1,$$

wenn a quadratischer Nichtrest von l ist, und nach der von Jacobi eingeführten erweiterten Definition dieses Symbols ist

(2) $$\left(\frac{a}{l\,l'\,l''\ldots}\right) = \left(\frac{a}{l}\right)\left(\frac{a}{l'}\right)\left(\frac{a}{l''}\right)\cdots$$

Ist ferner a ungerade, so ist

(3) $$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}},\quad \left(\frac{-2}{a}\right) = (-1)^{\frac{a^2-1}{8}},$$

und daraus, wenn $a, b, \ldots$ relativ prim zu m sind:

(4) $$\left(\frac{a}{m}\right)\left(\frac{b}{m}\right)\cdots = \left(\frac{a\,b\ldots}{m}\right);$$

ist D eine Diskriminante und a eine zu $2D$ teilerfremde Zahl, die durch eine Form φ der Diskriminante D eigentlich darstellbar ist, ferner l eine in D aufgehende ungerade Primzahl, so ist der Wert des Symbols $\left(\frac{a}{l}\right)$ nicht von der besonderen Zahl a, sondern nur von der Formenklasse A, zu der φ gehört, abhängig. Dasselbe gilt von

(5) $$\begin{array}{lll} \left(\frac{-1}{a}\right) & \text{mod}\quad D \equiv 0, -4 & (\text{mod } 16), \\ \left(\frac{2}{a}\right) & \qquad\quad D \equiv 0,\ \ 8 & \multirow{2}{*}{(\text{mod } 32).} \\ \left(\frac{-2}{a}\right) & \qquad\quad D \equiv 0, -8 & \end{array}$$

Hieraus lassen sich die Charaktere der Formenklassen zusammensetzen.

Wir werden bei einer späteren Anwendung den Fall besonders zu berücksichtigen haben, daß D durch 4 teilbar ist. Wir setzen daher:

(6) $$D = -4m\,^{1)},$$

und erhalten für diesen Fall, wenn $l, l', \ldots$ die verschiedenen in m aufgehenden ungeraden Primzahlen sind, die folgenden Charaktere:

[1]) Nach der Bezeichnung von Gauss: Formen erster Art der Determinante $-m$.

$$\left(\frac{a}{l}\right),\ \left(\frac{a}{l'}\right),\ \ldots \qquad m \equiv 3 \pmod 4,$$

$$\left(\frac{-1}{a}\right),\ \left(\frac{a}{l}\right),\ \left(\frac{a}{l'}\right),\ \ldots \qquad m \equiv 1 \pmod 4,$$

$$m \equiv 4 \pmod 8,$$

(7)
$$\left(\frac{2}{a}\right),\ \left(\frac{a}{l}\right),\ \left(\frac{a}{l'}\right),\ \ldots \qquad m \equiv 6 \pmod 8,$$

$$\left(\frac{-2}{a}\right),\ \left(\frac{a}{l}\right),\ \left(\frac{a}{l'}\right),\ \ldots \qquad m \equiv 2 \pmod 8,$$

$$\left(\frac{-1}{a}\right),\ \left(\frac{2}{a}\right),\ \left(\frac{a}{l}\right),\ \left(\frac{a}{l'}\right),\ \ldots \qquad m \equiv 0 \pmod 8.$$

Die Anzahl dieser Grundcharaktere ist, wie man sieht, gleich der in § 104, 3. näher bestimmten Zahl λ und die Anzahl der Vorzeichenkombinationen ist gleich 2^λ.

Die Abhängigkeit zwischen diesen Charakteren kann man so darstellen.

Ist

$$m = n^2 m', \quad D = Q^2 \Delta = -4 n^2 m'$$

und n^2 die größte in m aufgehende Quadratzahl, so ist

(8)
$$\Delta \equiv -m', \quad \text{wenn } m' \equiv 3 \pmod 4,$$
$$\Delta \equiv -4m' \quad \text{„} \quad m' \equiv 1, 2 \pmod 4;$$

im ersten Fall ist m' ungerade und nicht gleich 1, also gleich einer der Primzahlen l oder gleich einem Produkt aus mehreren von ihnen, und aus

$$\left(\frac{\Delta}{a}\right) = \left(\frac{-m'}{a}\right) = \left(\frac{a}{m'}\right) = 1,$$

worin das Reziprozitätsgesetz der quadratischen Reste angewandt ist, ergibt sich eine Relation zwischen den Charakteren.

Im zweiten Fall ist bei ungeradem m'

$$\left(\frac{-m'}{a}\right) = \left(\frac{-1}{a}\right)\left(\frac{a}{m'}\right) = 1,$$

und dies ist wieder ein Produkt mehrerer der Charaktere (7), und ist endlich $m' = 2m''$ gerade, so ist

$$\left(\frac{-m'}{a}\right) = \left(\frac{\pm 2}{a}\right)\left(\frac{a}{m''}\right),$$

wo das Zeichen $\pm$ so bestimmt wird, daß $\pm m'' \equiv 1 \pmod 4$ wird. Also ist wiederum die Anzahl der Geschlechter höchstens $= 2^{\lambda-1}$.

§ 106. Die Geschlechter der Idealklassen.

In § 100 haben wir gesehen, wie wir aus einer Zahlgruppe im Körper Ω Einteilungen der Ideale in Klassen ableiten können, und wie für diese Einteilungen die Klassenzahl zu bestimmen ist.

Wir wollen hier auch die Einteilung in Geschlechter aus diesem Gesichtspunkte betrachten.

Um unsere Betrachtungen gleich auf die Ordnungen ausdehnen zu können, scheiden wir von dem Gebiet der natürlichen Zahlen zunächst alle Zahlen aus, die mit irgend einer beliebig angenommenen Zahl S einen gemeinschaftlichen Teiler haben.

Hierauf nehmen wir einen positiven rationalen Modul m, und nehmen in S unter anderen alle Primzahlen auf, die in m enthalten sind.

Damit sind also alle Zahlen ausgeschieden, die einen gemeinschaftlichen Teiler mit m haben.

Aus den übrigbleibenden Zahlen und ihren Quotienten kann man eine Gruppe rationaler Brüche bilden, die wir mit Z bezeichnen wollen.

Ersetzen wir (nach Gauss) eine Zahl a^{-1} durch die ganze Zahl, die, mit a multipliziert, eine der Einheit kongruente Zahl ergibt, so können wir die Lehre von der Kongruenz nach dem Modul m ohne weiteres auf die gebrochenen Zahlen Z übertragen.

Sind dann a/b und a_1/b_1 Brüche in Z, so ist $a/b \equiv a_1/b_1$, wenn $a b_1 \equiv a_1 b$ im gewöhnlichen Sinne ist.

Vereinigen wir also alle untereinander kongruenten Zahlen in Z in eine Klasse, so zerfällt Z in $\varphi(m)$-Zahlklassen, deren jede durch eine ganze rationale Zahl repräsentiert werden kann.

Ist M die Gruppe der Zahlen a aus Z, die der Bedingung

$$a \equiv 1 \pmod{m}$$

genügen, so sind die Zahlklassen (modulo m) die Nebengruppen zu M, und es ist

$$(1) \qquad (Z, M) = \varphi(m).$$

Wir betrachten nun, wie im § 98, die Gruppen O der ganzen und gebrochenen Zahlen ω des quadratischen Körpers Ω, oder einer Ordnung $[Q]$ dieses Körpers, von denen wir alle

Zahlen ausschließen, die im Zähler oder im Nenner nicht relativ prim zu S sind. (Im Falle der Ordnungen müssen die Primfaktoren des Führers Q in S enthalten sein.)

Wir bilden nun aus M einen Teiler A, in den wir alle Zahlen a aufnehmen, die einer Kongruenz

(2) $$N(\omega) \equiv a \pmod{m}$$

genügen, d. h. für die eine Zahl ω in O existiert, deren Norm mit a kongruent ist.

1. Diese Zahlen heißen Normenreste für den Modul m.

Aus der Definition der Normenreste ergibt sich, daß die Normenreste der Multiplikation und Division gegenüber eine Gruppe bilden.

Ferner ergibt sich, daß jedes Quadrat und jeder quadratische Rest (modulo m) zugleich Normenrest ist, daß also jeder Normennichtrest zugleich quadratischer Nichtrest ist. Aus der Gruppennatur von A folgt:

Das Produkt aus Normenrest und Normenrest ist Normenrest.

Das Produkt aus Normenrest und Normennichtrest ist Normennichtrest.

Die Gruppe der Normenreste hat stets einen endlichen Index (Z, A), denn sie vereinigt in sich ganze Zahlklassen nach dem Modul m, deren Anzahl endlich ist.

§ 107. Zusammensetzung der Normenrestgruppen.

Wir wollen zwei Moduln m_1, m_2 betrachten, die zueinander relativ prim sind, und bezeichnen die Gruppen der Normenreste von m_1 und m_2 mit A_1 und A_2. Setzen wir für den Augenblick

$$(Z, A_1) = \mu$$

und zerlegen

(1) $$Z = a_1 A_1 + a_2 A_1 + \cdots + a_\mu A_1,$$

so können wir die $a_1, a_2, \ldots, a_\mu$ durch beliebige nach dem Modul m_1 kongruente Zahlen ersetzen. Da m_1 und m_2 relativ prim vorausgesetzt sind, so lassen sich, welches auch die rationalen Zahlen c_i seien, rationale x_i aus den Kongruenzen

$$a_i + x_i m_1 \equiv c_i \pmod{m_2}$$

bestimmen, und man kann also die a_i so wählen, daß sie in A_2 enthalten sind. Man kann also jede Zahl z in Z als Produkt

einer Zahl in A_1 mit einer Zahl in A_2 darstellen, was wir symbolisch durch

(2) $$Z = A_1 A_2$$

ausdrücken.

Der Durchschnitt A der Gruppen A_1 und A_2 enthält alle und nur die Zahlen, die zugleich Normenreste von m_1 und von m_2 sind, und wir beweisen, daß A die Gruppe der Normenreste m

(3) $$m = m_1 m_2$$

ist.

Ist nämlich a eine Zahl, die zugleich in A_1 und in A_2 enthalten ist, so gibt es zwei Zahlen ω_1, ω_2 in O, die den Bedingungen

(4) $$\begin{aligned} N(\omega_1) &\equiv a \pmod{m_1}, \\ N(\omega_2) &\equiv a \pmod{m_2} \end{aligned}$$

genügen. Es lassen sich nun zwei rationale Zahlen x_1, x_2 so bestimmen, daß

$$\begin{aligned} x_1 &\equiv 1 \pmod{m_1}, & x_2 &\equiv 0 \pmod{m_1}, \\ &\equiv 0 \pmod{m_2}, & &\equiv 1 \pmod{m_2}, \end{aligned}$$

und wenn wir dann also

$$\omega = x_1 \omega_1 + x_2 \omega_2$$

setzen, so ist

(5) $$\begin{aligned} N(\omega) &\equiv N(\omega_1) \equiv a \pmod{m_1}, \\ &\equiv N(\omega_2) \equiv a \pmod{m_2}, \end{aligned}$$

und da m_1 und m_2 relativ prim sind, so ist auch

(6) $$N(\omega) \equiv a \pmod{m},$$

also a Normenrest von m. Umgekehrt ist ein Normenrest von m zugleich Normenrest jedes Teilers von m, also auch von m_1 und m_2.

Hieraus ergibt sich nun mit Hilfe der Sätze 13. und 14., § 100:

$$\begin{aligned} (Z, A_1) &= (A_1 A_2, A_1) = (A_1 A_2, A_1 A) = (A_2, A), \\ (Z, A) &= (Z, A_2)(A_2, A) = (Z, A_1)(Z, A_2), \end{aligned}$$

und wir haben die Beziehung:

(7) $$(Z, A) = (Z, A_1)(Z, A_2).$$

Damit ist die Frage nach den Normenresten auf den Fall zurückgeführt, daß der Modul eine Primzahlpotenz ist.

§ 108. Normenreste der Primzahlpotenzen.

Es sei O eine Ordnungsgruppe im Körper Ω (§ 98) und P, die Gruppen der rationalen Zahlen, die relativ prim zur Diskri-

minante D dieser Ordnung und zugleich Normenreste einer Primzahl p in bezug auf diese Ordnung sind, d. h. der Zahlen a, die der Bedingung

$$(1) \qquad N(\omega) \equiv a \pmod{p}$$

für eine Zahl ω der Ordnung O genügen. Es gilt zunächst der Satz:

1. Wenn p nicht in D aufgeht, so ist jede Zahl a in Z Normenrest.

Es braucht dies nur bewiesen zu werden für den Fall, daß a ein quadratischer Nichtrest ist, da ja jeder quadratischer Rest zugleich Normenrest ist.

Es sei also $\mathfrak{p}$ ein in p aufgehendes Primideal des Körpers Ω.

Ist dann D quadratischer Rest von p, so ist $\mathfrak{p}$ vom ersten Grade (§ 92), und jede Zahl ist nach dem Modul $\mathfrak{p}$ mit einer rationalen Zahl kongruent.

Da p nicht in D aufgeht, so ist das zu $\mathfrak{p}$ konjugierte Ideal $\mathfrak{p}'$ von $\mathfrak{p}$ verschieden, und wir können eine Zahl ω in O finden, die den Kongruenzen:

$$\omega \equiv a \pmod{\mathfrak{p}}, \quad \equiv 1 \pmod{\mathfrak{p}'}\ ^{1)}$$

genügt (Bd. II, § 166). Ist dann ω' zu ω konjugiert, so ist

$$\omega \equiv a, \quad \omega' \equiv 1 \pmod{\mathfrak{p}},$$

und folglich

$$N(\omega) \equiv a \pmod{\mathfrak{p}}.$$

Ist aber D quadratischer Nichtrest von p, so ist $\mathfrak{p} = p$, und $D^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, folglich $\sqrt{D}^p \equiv -\sqrt{D}$ und für jede Zahl in O

$$(2) \qquad \begin{aligned} \omega^p &\equiv \omega' \pmod{p}, \\ N(\omega) &\equiv \omega^{p+1} \pmod{p}. \end{aligned}$$

Ist nun γ eine primitive Wurzel von p im Körper Ω, so ist $c \equiv \gamma^{p+1} \pmod{p}$ eine primitive Wurzel von p im Körper der rationalen Zahlen (Bd. II, § 167).

Setzen wir also

$$(3) \qquad a \equiv \gamma^{(p+1)x}, \quad \omega \equiv \gamma^x \pmod{p},$$

so ist nach (2) $N(\omega) \equiv a \pmod{p}$ und unser Satz somit bewiesen.

---

[1]) Setzt man $\omega = a + \xi\pi Q$, wo π eine durch $\mathfrak{p}$, aber nicht durch $\mathfrak{p}'$ teilbare Zahl ist, so kann man die Zahl ξ aus der Kongruenz $a + \xi\pi Q \equiv 1 \pmod{\mathfrak{p}'}$ bestimmen, und ω gehört wegen des Faktors Q zur Ordnung O.

2. Ist p eine in D aufgehende ungerade Primzahl, so ist a dann und nur dann Normenrest, wenn a quadratischer Rest von p ist.

Das ergibt sich unmittelbar aus der Bedingung für die Normenreste:

$$x^2 - Dy^2 \equiv 4a \pmod{p}, \tag{4}$$

die sich in diesem Fall auf $x^2 \equiv 4a \pmod{p}$ reduziert.

Die Primzahl 2 kommt nicht in Betracht, weil $x^2 \equiv a \pmod{2}$ immer lösbar ist, wohl aber die Moduln 4 und 8. Ist D ungerade, so ist $D \equiv 1 \pmod{4}$, und die Bedingung für einen Normenrest a ist:

$$\frac{x^2 - Dy^2}{4} \equiv a \quad (\text{mod } 4) \text{ oder } (\text{mod } 8),$$

und diese Kongruenz ist für jedes ungerade a lösbar (durch gerade x, y), also:

3. Geht 4 in D nicht auf, so ist jede ungerade Zahl a Normenrest von 4 und von 8.

Ist D durch 4 teilbar, so ist die Bedingung für einen Normenrest a die Möglichkeit der Kongruenz:

$$x^2 - \frac{D}{4} y^2 \equiv a \quad (\text{mod } 4) \text{ oder } (\text{mod } 8). \tag{5}$$

Da a ungerade ist, so können x und $Dy^2/4$ nicht beide ungerade sein.

Geht man hiernach die einzelnen Fälle durch, so ergibt sich

$\frac{D}{4} \equiv 0 \pmod{8}$, $a \equiv 1 \pmod{4}$, $a \equiv 1 \pmod{8}$,

$\frac{D}{4} \equiv 1 \pmod{8}$, keine Bedingung für a,

$\frac{D}{4} \equiv 2 \pmod{8}$, $a \equiv +1, -1 \pmod{8}$,

$\frac{D}{4} \equiv 3 \pmod{8}$, $a \equiv 1 \pmod{4}$, $a \equiv +1,\ 5 \pmod{8}$,

$\frac{D}{4} \equiv 4 \pmod{8}$, $a \equiv 1 \pmod{4}$, $a \equiv +1,\ 5 \pmod{8}$,

$\frac{D}{4} \equiv 5 \pmod{8}$, keine Bedingung für a,

$\frac{D}{4} \equiv 6 \pmod{8}$, $a \equiv +1,\ 3 \pmod{8}$,

$\frac{D}{4} \equiv 7 \pmod{8}$, $a \equiv 1 \pmod{4}$, $a \equiv +1,\ 5 \pmod{8}$.

Danach haben wir:

4. Ist $\frac{1}{4}D \equiv 1 \pmod 8$, so ist jede ungerade Zahl Normenrest von 4 und von 8.

Ist $\frac{1}{4}D \equiv 0 \pmod 8$, so sind nur die Zahlen von der Form $4n + 1$ Normenreste von 4 und die Zahlen der Form $8n + 1$ Normenreste von 8.

Ist $\frac{1}{4}D \equiv 2 \pmod 4$, so sind alle ungeraden Zahlen Normenreste von 4.

Ist $\frac{1}{4}D \equiv 2$, oder $\equiv 6 \pmod 8$, so sind im ersten Fall die Zahlen $8n + 1$, $8n - 1$, im zweiten Fall die Zahlen $8n + 1$, $8n + 3$ Normenreste von 8.

Ist $\frac{1}{4}D \equiv 3, 4, 7 \pmod 8$, so sind alle und nur die Zahlen der Form $4n + 1$ Normenreste von 4 und von 8.

5. Ist p eine ungerade Primzahl, und ein durch p nicht teilbares a Normenrest von p^k (für irgend einen positiven Exponenten k), so ist a auch Normenrest von p^{k+1}.

Zum Beweis sei

$$N(\omega) = a + p^k b,$$
$$\omega_1 = \omega(1 + xp^k),$$

worin x rational. Folglich

$$N(\omega_1) = (a + p^k b)(1 + xp^k)^2,$$
$$\equiv a + p^k(b + ax) \pmod{p^{k+1}},$$

und wenn x aus der Kongruenz $b + ax \equiv 0 \pmod p$ bestimmt wird, so folgt

$$N(\omega_1) \equiv a \pmod{p^{k+1}}.$$

6. Ist D ungerade, so gilt dasselbe auch noch für $p = 2$.

Denn in diesem Falle ist jedes ungerade a Normenrest von 8. Man setze also

$$N(\omega) = a + 2^k b, \qquad k \geqq 3,$$
$$\omega_1 = \omega\left(1 + 2^k x \frac{1 + \sqrt{D}}{2}\right),$$
$$N(\omega_1) \equiv (a + 2^k b)(1 + 2^k x) \pmod{2^{k+1}},$$

und wenn man $ax + b \equiv 0 \pmod 2$ annimmt, so folgt

$$N(\omega_1) \equiv a \pmod{2^{k+1}}.$$

7. Ist D gerade und a Normenrest von $2^k \geqq 8$, so ist a auch Normenrest von 2^{k+1}.

Denn man setze

$$N(\omega) = a + 2^k b,$$
$$\omega_1 = \omega(1 + 2^{k-1}x),$$

worin x rational. Dann ist $2k - 2 > k$, und folglich

$$N(\omega_1) \equiv (a + 2^k b)(1 + 2^k x) \pmod{2^{k+1}};$$
$$\equiv a + 2^k(b + ax);$$

wenn also

$$ax + b \equiv 0 \pmod 2,$$

so ist

$$N(\omega_1) \equiv a \pmod{2^{k+1}}.$$

Aus alledem ergibt sich nun folgender Satz:

8. Ist eine Zahl r in Z quadratischer Rest jeder in D aufgehenden ungeraden Primzahl, und ist außerdem bei geraden D

$$\text{a)} \begin{cases} r \equiv 1 \pmod 8 & \text{falls } \dfrac{D}{4} \equiv 0 \pmod 8, \\ r \equiv +1, -1 \pmod 8 & \quad \text{"} \quad \dfrac{D}{4} \equiv 2 \pmod 8, \\ r \equiv 1, 3 \pmod 8 & \quad \text{"} \quad \dfrac{D}{4} \equiv 6 \pmod 8, \end{cases}$$

$$\text{b)} \quad r \equiv +1, 5 \pmod 4 \qquad \text{"} \quad \frac{D}{4} \equiv 3, 4, 7 \pmod 8,$$

so ist r Normenrest von jedem beliebigen zu r teilerfremden Modul m.

Diese Zahlen r bilden eine Gruppe R, die wir die Gruppe der absoluten Normenreste nennen.

Ist b ein fester quadratischer Nichtrest der ungeraden Primzahl p, und z eine Zahl in Z, so ist entweder z oder $b^{-1}z$ in der Gruppe der Normenreste enthalten. Ist also P die Gruppe der Normenreste von p^k, so ist

$$(Z, P) = 1, \quad \text{wenn } p \text{ nicht in } D \text{ aufgeht},$$
$$(Z, P) = 2, \quad \text{wenn } p \text{ in } D \text{ aufgeht},$$

ferner, wenn L die Gruppe der Normenreste von 2^k ist:

$$(Z, L) = 1, \quad D \equiv 1 \pmod 4,$$
$$D \equiv 4, 20 \pmod{32},$$
$$(Z, L) = 2, \quad D \equiv 8, 12, 16, 24, 28 \pmod{32},$$
$$(Z, L) = 4, \quad D \equiv 0 \pmod{32}\text{ [1]}.$$

[1] Es ist nicht zu befürchten, daß das in § 99 und in Bd. II, § 21 erklärte Symbol (Z, P) für den Index eines Teilers einer Gruppe mit dem in § 85 ähnlich bezeichneten erweiterten Legendre-Jacobischen Symbol verwechselt werde.

9. Bezeichnen wir also mit ν die Anzahl der verschiedenen ungeraden in D aufgehenden Primzahlen, so ist nach § 98, 12.

$$(Z, R) = 2^{\nu}, \quad D \equiv 1 \pmod 4, \quad D \equiv 4 \pmod{16},$$
$$(Z, R) = 2^{\nu+1}, \quad D \equiv 8, 12, 16, 24, 28 \pmod{32},$$
$$(Z, R) = 2^{\nu+2}, \quad D \equiv 0 \pmod{32},$$

oder allgemein

$$(Z, R) = 2^{\lambda},$$

wo λ dieselbe Bedeutung hat wie in § 104, 3.

Diese Zahl stimmt, wie man sieht, mit der Anzahl der Stammteiler von D überein, und aus 8. folgt, daß ein absoluter Normenrest r diese Eigenschaft behält, wenn r um ein Vielfaches von D vermehrt wird.

Daraus der Satz:

10. Die absoluten Normenreste sind in einer endlichen Anzahl von arithmetischen Progressionen, die nach Vielfachen von D fortschreiten, enthalten.

Die in D aufgehenden ungeraden Primzahlen und in den Fällen a) und b) von Nr. 8 die Zahl 8 oder 4 heißen die charakteristischen Primzahlen und Primzahlpotenzen der Ordnung.

§ 109. Die Geschlechter der Ideale.

Nach dem Vorigen können wir die Gesamtheit der rationalen Zahlen z, mit Ausschluß derer, die zu D im Zähler oder Nenner nicht relativ prim sind, in μ Klassen (Nebengruppen) zerlegen, wobei

$$(Z, R) = \mu \tag{1}$$

der oben bestimmte Wert ist. Hiernach ist:

$$Z = R + R_1 + R_2 \ldots + R_{\mu-1}. \tag{2}$$

Wenn eine Zahl z in eine dieser Nebengruppen gehört, so gehören alle mit z nach dem Modul D kongruenten Zahlen in dieselbe Nebengruppe.

11. Die Hauptklasse R der Normenreste ist bei der Multiplikation und Division eine Gruppe.

Gehört r in die Hauptklasse R, so gehören zwei Zahlen z und rz in ein und dieselbe Klasse.

Die Gesamtheit der zu D teilerfremden ganzen und gebrochenen Ideale $\mathfrak{a}$ des Körpers Ω bilden auch eine Gruppe $\overline{O}$.

12. Wir teilen die Ideale $\mathfrak{a}$ in Geschlechter $G, G_1, G_2, \ldots$ ein, indem wir alle Ideale $\mathfrak{a}_\nu$, deren Normen $N(\mathfrak{a}_\nu)$ in einer Klasse R_ν enthalten sind, in ein Geschlecht G_ν vereinigen.

13. Die Ideale, deren Normen zugleich Normenreste r sind, gehören dem Hauptgeschlecht G an, und das Hauptgeschlecht ist selbst eine Gruppe.

Wollen wir gleich die Ordnungen berücksichtigen, so müssen wir auch Äquivalenz nach der Ordnung $[Q]$ zulassen (§ 100), was ja (für $Q = 1$) die allgemeine Äquivalenz einschließt. Dann gilt das Folgende:

14. Die Ideale der Hauptklasse gehören dem Hauptgeschlecht an, und äquivalente Ideale haben dasselbe Geschlecht.

Denn ist $\mathfrak{a}$ äquivalent mit $\mathfrak{a}_1$, so gibt es eine Zahl η in $[Q]$, für die $\mathfrak{a} = \eta\,\mathfrak{a}_1$ ist; folglich ist $N(\mathfrak{a}) = N(\eta)\,N(\mathfrak{a}_1)$ und $N(\eta)$ ist eine Zahl in R. Folglich gehören $\mathfrak{a}$ und $\mathfrak{a}_1$ nach 13. in dasselbe Geschlecht. Die Geschlechter umfassen daher nicht bloß die einzelnen Ideale, sondern die Idealklassen.

Damit eine Zahl a aus Z Idealnorm sein kann, ist eine gewisse Bedingung zu erfüllen. Ist nämlich

(3) $$a = N(\mathfrak{a}),$$

und zunächst $\mathfrak{a}$ ein primäres ganzes Ideal, so ist nach § 91

(4) $$\varDelta = b^2 - 4ac,$$

worin b, c ganze rationale Zahlen sind, und folglich ist

(5) $$(\varDelta, a) = +1.$$

Ist $\mathfrak{a}$ nicht primär, sondern gleich $m\,\mathfrak{a}_0$ mit primärem $\mathfrak{a}_0$, und $a_0 = N(\mathfrak{a}_0)$, so ist $a = m^2 a_0$, und folglich muß nach § 85, (15) auch hier die Bedingung (5) befriedigt sein, und das gleiche ergibt sich auch für gebrochene Zahlen, wenn Zähler und Nenner relativ prim zu D sind, wenn man in (5) a als ganzzahligen Repräsentanten seiner Klasse nach dem Modul D ansieht.

Da es nun Zahlen a gibt, für die $(\varDelta, a) = -1$ ist, so kann nicht jede Zahl in Z Norm eines Ideals sein, und die Anzahl der Geschlechter ist also kleiner als μ. Sie muß ein Teiler von μ, d. h. eine Potenz von 2 sein, und folglich haben wir den Satz:

15. Die Anzahl g der Geschlechter ist höchstens gleich

$$\tfrac{1}{2}\,(Z, R),$$

also der Hälfte der in 9. bestimmten Zahl.

Daß diese Zahl wirklich die genaue Anzahl der Geschlechter ist, werden wir später beweisen. Wir bemerken hierzu noch folgendes:

Die Tatsache, daß es für jedes Δ Zahlen a gibt, für die $(\Delta, a) = -1$ ist, folgt aus dem Reziprozitätsgesetze der quadratischen Reste. Kann man, ohne dieses Gesetz vorauszusetzen, die Existenz solcher Zahlen a nachweisen, so läßt sich umgekehrt dadurch ein Beweis des Reziprozitätsgesetzes ableiten. In dieser Weise hat Gauss seinen zweiten Beweis dieses Gesetzes hergeleitet. (Vgl. Dirichlet-Dedekind, § 152 ff.)

Ist r ein Normenrest und δ irgend ein Stammteiler von D, so ist

(6) $$N(\omega) = \frac{x^2 - y^2 D}{4} \equiv r \pmod{\delta}$$

und folglich, wenn r relativ prim zu δ ist,

(7) $$(\delta, r) = +1.$$

Für ungerade δ ist dies evident, für die geraden folgt es leicht in den verschiedenen Fällen von § 108. Wir setzen also allgemein, wenn z relativ prim zu D ist:

(8) $$\chi(z) = (\delta, z).$$

Dann ist $(\delta, r) = 1$ für jede Zahl r der Gruppe der absoluten Normenreste, und allgemein ist

(9) $$\chi(z)\chi(z_1) = \chi(z z_1).$$

Für alle Ideale $\mathfrak{a}$ des Hauptgeschlechtes, die zu D teilerfremd sind, ist

$$\chi[N(\mathfrak{a})] = +1,$$

und daraus folgt, daß $\chi[N(\mathfrak{a})]$ für alle Ideale $\mathfrak{a}$ eines Geschlechtes einen und denselben Wert $\chi(G)$ hat.

Diese Funktionen sind also die Charaktere der Gruppe der Geschlechter.

Sechzehnter Abschnitt.

Klassenzahl in quadratischen Körpern.

---

§ 110. Fundamentale Einheiten in den Ordnungen.

Die Theorie der Einheiten, die wir allgemein in Bd. II, § 191 auseinandergesetzt haben, nimmt für die quadratischen Körper eine einfachere Gestalt an, muß aber andererseits erweitert und für die Ordnungen ausgebildet werden.

Die ganzen Zahlen der Ordnung O mit der Diskriminante D sind nach § 96, (6) in der Form $x_1 + x_2\theta$ enthalten, worin

$$\theta = \tfrac{1}{2}\sqrt{D}, \qquad \text{wenn } D \equiv 0 \pmod 4,$$

$$\theta = \frac{1+\sqrt{D}}{2}, \qquad \text{„} \quad D \equiv 1 \pmod 4,$$

und x_1, x_2 ganze rationale Zahlen sind.

Eine solche Zahl ε ist eine Einheit, wenn

(1) $$N(\varepsilon) = (x_1 + x_2\theta)(x_1 + x_2\theta') = \pm 1$$

ist. Hierfür ergibt sich die Bedingung

(2) $$x_1^2 - x_2^2 D = \pm 4.$$

Ist D negativ, so kann hier nur das positive Zeichen stehen, und es gibt im allgemeinen nur die zwei Lösungen $x = \pm 2$, $y = 0$ und in den beiden Ausnahmefällen die vier oder sechs Lösungen:

$$\begin{array}{lll} D = -4, & x_1 = \pm 2, & x_2 = 0, \\ & x_1 = 0, & x_2 = \pm 1. \\ D = -3, & x_1 = \pm 2, & x_2 = 0, \\ & x_1 = \pm 1, & x_2 = \pm 1. \end{array}$$

Daraus folgt:

1. Für ein negatives D gibt es im allgemeinen nur die zwei Einheiten

$$\varepsilon = +1, \qquad \varepsilon = -1,$$

und für zwei besondere Fälle

$$D = -4: \ \varepsilon = +1, \ -1, \ +i, \ -i,$$

$$D = -3: \ \varepsilon = +1, \ -1,$$

$$-\frac{1+\sqrt{-3}}{2}, \ -\frac{1-\sqrt{-3}}{2}, \ +\frac{1+\sqrt{-3}}{2}, \ +\frac{1-\sqrt{-3}}{2}.$$

Die von Null verschiedenen Zahlen der Ordnung O sind dann zu je zwei oder in den beiden Ausnahmefällen zu je vier oder zu je sechs assoziiert.

2. Ist D positiv, so gibt es eine Lösung der Pellschen Gleichung:

$$T^2 - U^2 D = \pm 4,$$

in der T und U positive und möglichst kleine Werte haben. Ist dann

$$\varepsilon = \frac{T + U\sqrt{D}}{2},$$

so sind alle Einheiten in der Form $\pm \varepsilon^{\pm \nu}$ enthalten, wo ν die Reihe der Zahlen 0, 1, 2, ... durchläuft.

Ist die Gleichung (2) für das negative Zeichen lösbar, so ist $N(\varepsilon) = -1$, und es hat $\pm \varepsilon^{\nu}$ für gerade ν eine positive, für ungerade ν eine negative Norm. Ist aber (2) nur für das obere Zeichen lösbar, so haben alle Einheiten positive Norm. Unter den Zahlen y der Ordnung O, die nicht Einheiten sind, gibt es aber immer solche mit negativer Norm.

Ist $N(\varepsilon) = -1$, so gibt es zu jeder Zahl y in O mit negativer Norm eine assoziierte mit positiver Norm. Ist aber $N(\varepsilon) = +1$, so zerfallen die Zahlen y in zwei Klassen, von denen die eine positive und die andere negative Norm hat, und keine Zahl der einen Klasse ist mit einer der anderen Klasse assoziiert.

Demgemäß betrachten wir nur die Zahlen y der Ordnung O mit positiver Norm, unter denen y und $\pm \varepsilon^{\pm \nu} y$ nur dann assoziiert sind, wenn

$$\varepsilon = \frac{T + U\sqrt{D}}{2}$$

die fundamentale Einheit mit positiver Norm, also T, U die kleinste positive Lösung von

$$T^2 - U^2 D = +4 \tag{3}$$

ist.

Bei positiver Diskriminante gibt es unendliche Scharen assoziierter Zahlen, und es kommt darauf an, durch eine passende Bestimmung von jeder dieser Scharen eine bestimmte auszusondern. Dazu bieten uns die allgemeinen Betrachtungen von Bd. II, § 195 die Hilfsmittel, die wir jetzt auf unseren speziellen Fall anwenden.

Es sei nach § 98

$$\lambda = a t_1 + \frac{b + \sqrt{D}}{2} t_2$$

eine Basisform in der Ordnung $[Q]$ eines Ideals $\mathfrak{a}$, das wir primär voraussetzen wollen und

$$\begin{aligned} y &= a x_1 + \frac{b + \sqrt{D}}{2} x_2 \\ y' &= a x_1 + \frac{b - \sqrt{D}}{2} x_2 \end{aligned} \tag{4}$$

mit ganzen rationalen x_1, x_2 eine durch $\mathfrak{a}$ teilbare ganze Zahl y in $[Q]$ mit positiver Norm nebst ihrer Konjugierten y', und da wir $\mathfrak{a}$ als primär vorausgesetzt haben, so ist

$$a = N(\mathfrak{a}). \tag{5}$$

Es sei ferner

$$\begin{aligned} \varepsilon &= \frac{T + U\sqrt{D}}{2}, \\ \varepsilon' &= \frac{T - U\sqrt{D}}{2} \end{aligned} \tag{6}$$

die fundamentale Einheit in O mit ihrer Konjugierten, die beide positiv sind und positive Norm haben.

Wir bestimmen die Zahlen ξ_1 und ξ_2 aus den linearen Gleichungen:

$$\begin{aligned} \xi_1 \log \varepsilon + \xi_2 &= \log |y|, \\ \xi_1 \log \varepsilon' + \xi_2 &= \log |y'|, \\ \xi_1 \log \frac{\varepsilon}{\varepsilon'} &= \log \left| \frac{y}{y'} \right|, \\ \xi_2 &= \tfrac{1}{2} \log |y y'|, \end{aligned} \tag{7}$$

worin $|y|$ den absoluten Wert von y bedeutet.

Ersetzt man y durch eine assoziierte Zahl $\pm \varepsilon^k y$, so geht ξ_1 in $\xi_1 + k$ über, worin k eine positive oder negative ganze Zahl ist, und man kann also y unter den Assoziierten immer auf eine Weise so wählen, daß

$$(8) \qquad 0 \lesseqgtr \xi_1 < 1$$

wird. Die so bestimmte Zahl y ist dann die reduzierte Zahl.

Beachtet man noch, daß die Gleichungen (7) sich nicht ändern, wenn y durch $-y$ ersetzt wird, so folgt:

3. In einer Schar assoziierter Zahlen gibt es immer zwei und nur zwei reduzierte Zahlen, die sich nur im Vorzeichen unterscheiden.

Aus (7) ergibt sich, wenn ξ_1 der Bedingung (8) genügt:

$$(9) \qquad 0 \leqq \log \left|\frac{y}{y'}\right| < \log \frac{\varepsilon}{\varepsilon'},$$

und daraus

$$(10) \qquad 1 \leqq \left|\frac{y}{y'}\right| < \frac{\varepsilon}{\varepsilon'},$$

und umgekehrt folgen aus (10) wieder die Gleichungen (7) mit der Bedingung (8).

Da wir überdies vorausgesetzt haben, daß y eine positive Norm haben soll, so haben y, y' das gleiche Vorzeichen, und dieses ist positiv, wenn x_2 positiv ist. Denn dann ist $y - y' = x_2 \sqrt{D}$ positiv, und da $|y| > |y'|$ ist, so müssen y und y' positiv sein.

In dem besonderen Falle $x_2 = 0$ ist y und y' positiv, wenn wir x_1 positiv voraussetzen. Damit ist dann die in 3. noch übriggebliebene Zweideutigkeit beseitigt.

Da also y und y' positiv sind, so folgt aus (10):

$$(11) \qquad y'\varepsilon - y\varepsilon' > 0.$$

Woraus nach (4) und (6):

$$(12) \qquad 2aUx_1 - (T - bU)x_2 > 0, \quad x_2 \geqq 0.$$

Und diese Bedingungen, die wir die Isolierungsbedingungen nennen, schließen bereits in sich, daß y' und folglich $N(y)$ positiv ist. Denn nach (3) ist

$$T > U\sqrt{D},$$

und demnach folgt aus (12):

$$U[2ax_1 + (b - \sqrt{D})x_2] > 0.$$

Damit ist bewiesen:

4. Ist $\mathfrak{a}$ ein zu Q teilerfremdes Ideal, so liefert u
jedes den Bedingungen (12) genügende Zahlenpaar x_1,
eine durch $\mathfrak{a}$ teilbare positive Zahl y mit positiver Nor
der Ordnung $[Q]$

$$y = a x_1 + \frac{b + \sqrt{D}}{2} x_2, \tag{13}$$

und unter diesen Zahlen sind keine zwei assoziiert.

§ 111. Die Dirichletsche Grenzformel.

Bedeutet t eine positive Konstante, so ist durch die Bedingung:

$$N(y) = a(a x_1^2 + b x_1 x_2 + c x_2^2) \lesseqgtr t, \tag{1}$$

und, bei positiver Diskriminante, durch die Isolierungsbedingungen, in einer Ebene, in der x_1, x_2 rechtwinkelige Koordinaten sind, ein Gebiet F_t begrenzt, das bei negativer Diskriminante durch eine Ellipse, bei positiver Diskriminante durch einen Hyperbelbogen und durch gerade Linien begrenzt ist. Die Punkte, deren Koordinaten x_1, x_2 ganze rationale Zahlen sind, heißen Gitterpunkte.

Einem ganzen System von assoziierten Zahlen, deren Norm positiv und kleiner als t ist, entspricht dann bei positiver Diskriminante ein Gitterpunkt in F_t und bei negativer Diskriminante zwei und in den beiden Ausnahmefällen vier und sechs Gitterpunkte.

Bezeichnet Z_t die Anzahl der Gitterpunkte in dem Gebiete F_t und V die Fläche des Gebietes F_t, so ist [Bd. II, § 194, (6)]:

$$V = Z_t t^{-1} + R_t t^{-\frac{1}{2}}, \tag{2}$$

worin R_t mit unendlich wachsendem t nicht unendlich wird.

Bei negativer Diskriminante erhält man V aus dem bekannten Flächeninhalt der Ellipse:

$$V = \frac{2\pi}{a\sqrt{-D}}, \tag{3}$$

und bei positiver Diskriminante erhält man ihn am einfachsten, indem man nach § 110, (7) an Stelle von x_1, x_2 die Integrationsvariablen ξ_1, ξ_2 einführt, deren Grenzen $0, 1$ und $-\infty, 0$ sind:

$$V = \frac{\log \varepsilon}{a\sqrt{D}}. \tag{4}$$

Hiernach ergibt sich aus (2):

$$(5)\qquad \operatorname*{Lim}_{t=\infty} \frac{Z_t}{t} = \frac{\log \varepsilon}{a\sqrt{D}}, \qquad D > 0,$$

$$= \frac{2\pi}{a\sqrt{-D}}, \qquad D < 0.$$

Nach Bd. II, § 196, 4. ist aber

$$\operatorname*{Lim}_{s=1} \sum \frac{s-1}{(Ny)^s} = \operatorname*{Lim}_{t=\infty} \frac{Z_t}{t},$$

und es ergibt sich also aus (5):

$$(6)\qquad \operatorname*{Lim}_{s=1} \sum \frac{s-1}{(Ny)^s} = \frac{1}{a\sqrt{D}} \log \varepsilon, \qquad D > 0,$$

$$= \frac{2\pi}{a\sqrt{-D}}, \qquad D < 0.$$

Hier durchläuft y die Reihe der ganzen Zahlen der Ordnung $[Q]$, die durch ein zu Q teilerfremdes primäres Ideal $\mathfrak{a}$ teilbar sind, wobei jedoch von einer Schar assoziierter Zahlen immer nur ein Repräsentant, der jetzt beliebig gewählt sein kann, beizubehalten ist (bei negativen D zwei oder vier oder sechs).

Hierbei sind unter assoziierten Zahlen (nach der Ordnung $[Q]$) solche zu verstehen, deren Quotient eine Einheit der Ordnung Q ist.

Wir wollen jetzt von den Zahlen y noch alle die ausschließen, die nicht relativ prim zu Q sind. Dann modifiziert sich die Summe (6) in folgender Weise: Ist r ein Primfaktor von Q, so sind alle Zahlen der Ordnung $[Q]$, die zu r nicht teilerfremd sind, durch r teilbar, weil sie ja nach dem Modul r mit einer rationalen Zahl kongruent sind.

Setzen wir also

$$(7)\qquad y = r y_1,$$

so ist y_1 durch $\mathfrak{a}$ teilbar, braucht aber nicht der Ordnung $[Q]$, sondern nur der Ordnung $\left[\frac{Q}{r}\right] = [Q_1]$ anzugehören. Ist bei positiver Diskriminante ε_1 die fundamentale Einheit der Ordnung $[Q_1]$, so ist

$$(8)\qquad \varepsilon = \varepsilon_1^\lambda$$

eine Potenz von ε_1, und es ist $\sqrt{D} = r\sqrt{D_1}$. Die Zahlen

$$(9)\qquad y = r y_1 \varepsilon_1^t, \quad t = 0, 1, 2, \ldots, \lambda - 1$$

haben alle dieselbe Norm; sie sind assoziiert nach $[Q_1]$, aber nicht nach $[Q]$. Demnach erhalten wir nach (6):

$$\operatorname*{Lim}_{s=1} \sum \frac{s-1}{(N y_1)^s} = \frac{r}{a\sqrt{D}} \frac{\log \varepsilon}{\lambda};$$

um daraus die auf die Zahlen (9) bezügliche Summe zu erhalten, hat man, da $N(\varepsilon_1) = 1$, $N(r) = r^2$ ist, mit λ zu multiplizieren und mit r^2 zu dividieren. Man erhält so:

$$\operatorname{Lim} \sum \frac{s-1}{(N y)^s} = \frac{1}{r a \sqrt{D}} \log \varepsilon.$$

Zieht man dies von der Summe (6) ab und verfährt ebenso mit allen Primfaktoren r von Q, so ergibt sich:

$$(10) \quad \operatorname{Lim} \sum \frac{s-1}{(N y)^s} = \prod \left(1 - \frac{1}{r}\right) \frac{1}{a\sqrt{D}} \log \varepsilon, \qquad D > 0,$$

und noch einfacher bei negativer Diskriminante:

$$= \prod \left(1 - \frac{1}{r}\right) \frac{\pi}{a\sqrt{-D}}, \qquad D < 0,$$

worin sich die Summe nur auf die Zahlen y erstreckt, die zu Q teilerfremd sind, und das Produkt Π sich auf alle Primfaktoren von r bezieht. Nur in den beiden Ausnahmefällen $D = -4$, $D = -3$ ist die rechte Seite der letzten Formel noch durch 2 oder durch 3 zu dividieren.

Zerlegt man y in Idealfaktoren

$$(11) \qquad y = \mathfrak{a}\mathfrak{m},$$

so durchläuft $\mathfrak{m}$ alle Ideale einer bestimmten Idealklasse nach der Ordnung $[Q]$, die zu Q teilerfremd sind. Diese Klasse ist, wenn $\mathfrak{a}$ in die Klasse A gehört,

$$M = A^{-1},$$

und unter den Zahlen

$$N(y) = a N(\mathfrak{m})$$

kommt im Falle der positiven Diskriminante jedes $N(\mathfrak{m})$ nur einmal, im Falle einer negativen Diskriminante zwei- oder vier- oder sechsmal vor.

Demnach ergibt sich aus (10):

$$(12) \qquad \operatorname*{Lim}_{s=1} \sum \frac{s-1}{(N\mathfrak{m})^s} = \prod \left(1 - \frac{1}{r}\right) \frac{1}{\sqrt{D}} \log \varepsilon, \quad D > 0$$

$$= \prod \left(1 - \frac{1}{r}\right) \frac{\pi}{\sqrt{-D}}, \quad D < 0$$

und in den beiden Ausnahmefällen $D = -4$, $D = -3$ ist der letzte Ausdruck durch 2 oder durch 3 zu dividieren.

Es durchläuft hierin $\mathfrak{m}$ die Gesamtheit der Ideale einer Klasse (nach $[Q]$), und man sieht, daß dieser Grenzwert von dieser besonderen Klasse nicht abhängig ist.

Es ist bisweilen zweckmäßig, in der Summe auf der linken Seite der Formel (12) nicht bloß solche Ideale von $\mathfrak{m}$ auszuschließen, die mit Q einen Teiler gemein haben, sondern auch die, die nicht teilerfremd zu Δ sind. Die Formel (12) gilt unter dieser Voraussetzung unverändert, wenn man unter den r der rechten Seite nicht nur die Primteiler von Q, sondern alle Primteiler von D versteht.

Ist nämlich $\mathfrak{r}$ ein in D, aber nicht in Q aufgehendes Primideal, so ist $N(\mathfrak{r}) = r_1$ eine in D, aber nicht in Q aufgehende natürliche Primzahl, und es ist $N(\mathfrak{r}\mathfrak{m}) = r_1 N(\mathfrak{m})$. Nimmt man also von der Summe der linken Seite von y die den $\mathfrak{r}\mathfrak{m}$ entsprechenden Glieder noch weg, so kommt rechts der Faktor $\left(1 - \frac{1}{r_1}\right)$ hinzu.

5. Der Grenzwert in der Formel (12) ist nur von der Diskriminante D, nicht von der besonderen Klasse M abhängig und ist stets von Null verschieden.

§ 112. Klassenzahl.

Wir nehmen nun eine Funktion $F(z)$ an, die übrigens nur für ganzzahlige Werte von z definiert zu sein braucht, von der wir voraussetzen, daß die unendliche Reihe

(1) $$\sum^{\mathfrak{a}} F(N\mathfrak{a}),$$

in der $\mathfrak{a}$ die Gesamtheit der Ideale des Körpers Ω (oder nur einen Teil davon) durchläuft, unbedingt konvergent sei. Wir wollen, wenn es sich um Ordnungen $[Q]$ handelt, von $\mathfrak{a}$ alle die ausschließen, die nicht relativ prim zu Q sind.

Irgend eine natürliche zu Q teilerfremde Zahl m kommt dann unter den $N(\mathfrak{a})$ nach § 93, 4.

$$\sum^{n} (\Delta, n)$$

mal vor, wenn n die Teiler von m durchläuft, und wir erhalten die Formel:

(2) $$\sum F(N\mathfrak{a}) = \sum^{m}\sum^{n} (\Delta, n) F(m),$$

worin m alle positiven ganzen Zahlen, die zu Q relativ prim sind, und n für jedes m die Teiler von m durchläuft.

Ordnen wir auf der rechten Seite von (2) nach n, so kommen für ein gegebenes n unter den m alle Vielfachen von n vor, und wir können auch setzen:

$$(3) \qquad \Sigma F(N\mathfrak{a}) = \overset{m}{\Sigma}\overset{n}{\Sigma}(\Delta, n) F(mn),$$

worin jetzt m und n, voneinander unabhängig, alle natürlichen Zahlenwerte annehmen, die mit Q keinen Teiler gemein haben.

Ist im besonderen F so beschaffen, daß

$$(4) \qquad F(mn) = F(m) F(n)$$

ist, so können wir (3) auch so darstellen:

$$(5) \qquad \overset{\mathfrak{a}}{\Sigma} F(N\mathfrak{a}) = \overset{m}{\Sigma} F(m) \overset{n}{\Sigma}(\Delta, n) F(n).$$

Bei den Summen nach m und n sind die Zahlen ausgeschlossen, die mit Q einen Teiler gemein haben.

Ebenso sind auf der linken Seite die Ideale ausgeschlossen, die zu Q nicht relativ prim sind.

Die Formel (5) können wir zunächst anwenden, um aus den Formeln des vorigen Paragraphen die Klassenzahl zu bestimmen. Man erhält auf diese Weise auch das Verhältnis der Klassenzahl im Körper zu der Klassenzahl nach der Ordnung $[Q]$. Da wir dieses Verhältnis aber schon auf anderem Wege bestimmt haben (§ 100), so wollen wir uns hier auf die Klassenzahl des Körpers beschränken, d. h. wir wollen $Q = 1$ setzen.

Setzen wir in (5) $F(z) = z^{-s}$, so findet die vorausgesetzte unbedingte Konvergenz statt, solange $s > 1$ ist. Multiplizieren wir aber mit $s - 1$ und lassen s in 1 übergehen, so können wir von § 111, (12) Gebrauch machen.

Diese Formel wenden wir in der ersten Fassung an, bei der $\mathfrak{m}$ die zu Q teilerfremden Ideale der Klasse M durchläuft und r die Primfaktoren von Q bedeuten. Diese fallen also für $Q = 1$ ganz weg, und $\mathfrak{m}$ ist in der Summenformel:

$$(6) \qquad \sum \frac{s-1}{(N\mathfrak{m})^s} = \frac{1}{\sqrt{\Delta}} \log \varepsilon, \qquad \Delta > 0$$

$$= \frac{\pi}{\sqrt{-\Delta}}, \qquad \Delta < 0$$

keiner Beschränkung in bezug auf Teilbarkeit mehr unterworfen.

Jeder Teil der Summe auf der linken Seite der Formel (5), der sich auf eine Idealklasse bezieht, gibt dann denselben Beitrag zu der Summe, und wir erhalten:

$$(7) \qquad \operatorname*{Lim}_{s=1}(s-1)\sum\frac{1}{m^s}\sum\frac{(\Delta,n)}{n^s} = h\frac{1}{\sqrt{\Delta}}\log\varepsilon, \qquad \Delta > 0$$

$$= h\frac{\pi}{\sqrt{-\Delta}}, \qquad \Delta < 0.$$

Hier ist h die Klassenzahl des Körpers Ω, und um nicht immer wieder die beiden Ausnahmefälle $\Delta = -4$, $\Delta = -3$ anführen zu müssen, wollen wir festsetzen, daß in diesen beiden Fällen, in denen die Klassenzahl 1 ist, unter h der Wert $\frac{1}{2}$ oder $\frac{1}{3}$ verstanden werden soll.

So oft n ein volles Restsystem nach dem Modul Δ durchläuft, ist $\Sigma(\Delta, n) = 0$ [§ 85, (22)], und folglich bleibt die Summe $\Sigma(\Delta, n)$, wenn die n der Größe nach geordnet sind, wie weit auch n wächst, immer endlich. Danach ist der Satz Bd. II, § 196, 1. anwendbar, nach dem

$$\operatorname*{Lim}_{s=1}\sum\frac{(\Delta,n)}{n^s} = \sum\frac{(\Delta,n)}{n}$$

ist. Andererseits ist

$$\operatorname{Lim}(s-1)\Sigma\frac{1}{m^s} = 1$$

(Bd. II, § 196, S. 723), und es ergibt sich aus (7):

$$(8) \qquad \begin{aligned} h\log\varepsilon &= \sqrt{\Delta}\sum_{1,\infty}^{n}\frac{(\Delta,n)}{n}, \qquad \Delta > 0 \\ h\pi &= \sqrt{-\Delta}\sum_{1,\infty}^{n}\frac{(\Delta,n)}{n}, \qquad \Delta < 0. \end{aligned}$$

Die Summe

$$\sigma = \Sigma\frac{(\Delta,n)}{n}$$

läßt sich in endlicher Form darstellen. Es ist nämlich nach § 86, (2):

$$(9) \qquad \sqrt{\Delta}\,(\Delta,n) = \overset{k}{\Sigma}(\Delta,k)\,e^{-\frac{2nk\pi i}{\Delta}},$$

worin k ein vollständiges Restsystem nach dem Modul Δ durchläuft und bei negativer Diskriminante $\sqrt{\Delta} = i\sqrt{-\Delta}$ zu setzen ist. Danach folgt:

$$\sigma = \frac{1}{\sqrt{\Delta}}\sum^{k}(\Delta,k)\sum^{n}\frac{1}{n}e^{-\frac{2nk\pi i}{\Delta}},$$

und da σ reell ist:

$$\Delta > 0. \qquad \sigma = \frac{1}{\sqrt{\Delta}} \sum^{k} (\Delta, k) \sum^{n} \frac{1}{n} \cos \frac{2nk\pi}{\Delta},$$

$$\Delta < 0. \qquad \sigma = \frac{1}{\sqrt{-\Delta}} \sum^{k} (\Delta, k) \sum^{n} \frac{1}{n} \sin \frac{mk\pi}{-\Delta}.$$

Die beiden unendlichen Reihen nach n haben aber bestimmte Werte, die Abel in der Abhandlung über die Binomialreihe aus der Potenzwickelung von $\log(1 - z)$ abgeleitet hat, und die sich auch aus der Theorie der Fourierschen Reihen ergeben. Wird dann k positiv und zwischen 0 und $\pm\Delta$ genommen, so ergibt sich:

$$\sum \frac{1}{n} \cos \frac{2nk\pi}{\Delta} = -\log\left(2 \sin \frac{k\pi}{\Delta}\right),$$

$$\sum \frac{1}{n} \sin \frac{2nk\pi}{-\Delta} = \frac{\pi}{2}\left(1 - \frac{2k}{-\Delta}\right).$$

Also ergibt sich aus (8) [mit Rücksicht auf $\Sigma(\Delta, k) = 0$]:

$$(10) \qquad \begin{aligned} h \log \varepsilon &= -\overset{k}{\Sigma}(\Delta, k) \log \sin \frac{k\pi}{\Delta}, & \Delta > 0, \\ h &= \frac{1}{\Delta} \overset{k}{\Sigma}(\Delta, k) k, & \Delta < 0. \end{aligned}$$

Für den Fall der negativen Diskriminante kann man den Ausdruck für h so umgestalten, daß er die Form einer ganzen Zahl annimmt.

Ist zunächst Δ ungerade ($\equiv 1 \bmod 4$), so kann man die Zahlenreihe k so zerlegen:

$$\begin{matrix} \nu, & -\Delta - \nu, \\ 2\nu, & -\Delta - 2\nu, \end{matrix} \qquad 0 < \nu < -\frac{\Delta}{2},$$

und erhält also, da hier $(\Delta, -\nu) = -(\Delta, \nu)$ ist (§ 85), zwei Formen des Ausdrucks h:

$$h = \frac{2}{\Delta} \overset{\nu}{\Sigma}(\Delta, \nu)\nu + \overset{\nu}{\Sigma}(\Delta, \nu),$$

$$h = \frac{4}{\Delta} \Sigma(\Delta, 2\nu)\nu + \overset{\nu}{\Sigma}(\Delta, \nu),$$

woraus, wenn man die erste mit 2, die zweite mit $(\Delta, 2)$ multipliziert und subtrahiert:

$$(11) \qquad [2 - (\Delta, 2)]h = \overset{\nu}{\Sigma}(\Delta, \nu).$$

Wenn also $(\Delta, 2) = -1$ ist, so muß die rechte Seite durch 3 teilbar sein.

Für den Fall eines geraden Δ zerlegt man k in

$$\nu, \quad -\frac{\Delta}{2}+\nu, \qquad 0<\nu<\frac{\Delta}{2}$$

und wendet die Formel an:

$$\left(\Delta, \; -\frac{\Delta}{2}+\nu\right) = -(\Delta,\nu),$$

die sich aus den Sätzen des § 85 leicht ergibt.

Dann findet man zunächst:

$$h = \tfrac{1}{2}\sum^{\nu}(\Delta,\nu),$$

und wenn man die ν nochmals zerlegt in

(12) $$\mu, \quad -\frac{\Delta}{2}-\mu: \qquad 0<\mu\leqq\frac{-\Delta}{4},$$
$$h = \Sigma(\Delta,\mu).$$

Die Formel für positive Diskriminanten läßt sich mit Hilfe der Kreisteilungstheorie umformen, worauf wir hier nicht eingehen wollen.

§ 113. Die Anzahl der Geschlechter.

Die Formel (5) des vorigen Paragraphen gestattet die Bestimmung der genauen Anzahl der Geschlechter nach Dirichlet. Wir verstehen unter δ irgend einen Stammteiler von D und setzen:

(1) $$F(z) = \frac{(\delta,z)}{z^s}, \text{ wo } z \text{ relativ prim zu } D \text{ ist,}$$
$$F(z) = 0, \qquad \text{wenn } z \text{ und } D \text{ einen gemeinsamen Teiler haben.}$$

Dann ist $(\delta, N\mathfrak{a})$ einer der Charaktere des durch $\mathfrak{a}$ bestimmten Geschlechtes. Bezeichnen wir diesen Charakter also mit (δ, A), so folgt aus § 112, (5):

(2) $$\sum^{A}(\delta,A)\sum^{\mathfrak{a}}\frac{1}{(N\mathfrak{a})^s} = \sum\frac{(\delta,m)}{m^s}\sum\frac{(\delta',n)}{n^s}.$$

Darin ist $\delta' = \delta\Delta$ und kann, da n relativ prim zu D ist, auch durch den Stamm von $\delta\Delta$ ersetzt werden (nach der symbolischen Multiplikation in § 104). Ist $\delta = 1$, so ist $\delta' = \Delta$, und ist $\delta = \Delta$, so ist $\delta' = 1$.

Von den beiden Fällen $\delta = 1$, $\delta = \Delta$ abgesehen, behalten also die Summen auf der rechten Seite von (2) für $s = 1$ einen endlichen Wert (die nach dem vorigen Paragraphen durch Klassenzahlen der Diskriminanten δ, δ' ausdrückbar sind).

Auf der linken Seite von (2) durchläuft in der Summe nach $\mathfrak{a}$ das Zeichen $\mathfrak{a}$ die Gesamtheit der Ideale der einzelnen Klassen,

und die Summe $\sum^{\mathfrak{a}} \frac{s-1}{(N\mathfrak{a})^s}$, über eine Klasse A ausgedehnt, hat für $s = 1$ einen bestimmten von Null verschiedenen Grenzwert, der nach § 111, 5. für alle Klassen der gleiche ist. Daraus folgt nach 2.:

$$\overset{A}{\Sigma}(\delta, A) = 0, \tag{3}$$

außer wenn $\delta = 1$ oder $= \Delta$ ist,

$$\overset{A}{\Sigma}(\delta, A) = h, \tag{4}$$

wenn $\delta = 1$ oder $= \Delta$ ist [weil $(\Delta, A) = 1$, § 104, (10)].

Ferner ist für jede Klasse A_0 des Hauptgeschlechts $(\delta, A_0) = 1$, während es für jede Klasse A, die nicht dem Hauptgeschlecht angehört, wenigstens ein δ_1 gibt, so daß $(\delta_1, A) = -1$ ist. Daraus folgt, wenn 2^ν die Anzahl der Stammteiler ist,

$$\overset{\delta}{\Sigma}(\delta, A_0) = 2^\nu, \tag{5}$$

$$(\delta_1, A) \overset{\delta}{\Sigma}(\delta, A) = \overset{\delta}{\Sigma}(\delta\,\delta_1, A),$$

und da $\delta\,\delta_1$ zugleich mit δ die Gesamtheit der Stammteiler durchläuft (wenn man $\delta\,\delta_1$ nach der symbolischen Multiplikation in § 104 reduziert):

$$(\delta_1, A) \overset{\delta}{\Sigma}(\delta, A) = \overset{\delta}{\Sigma}(\delta, A),$$

und wenn also $(\delta_1, A) = -1$ ist:

$$\overset{\delta}{\Sigma}(\delta, A) = 0. \tag{6}$$

Hiernach können wir die Doppelsumme

$$\overset{\delta}{\Sigma}\overset{A}{\Sigma}(\delta, A)$$

auf zwei Arten bestimmen. Es ergibt sich nach (3), (4):

$$\overset{\delta}{\Sigma}\overset{A}{\Sigma}(\delta, A) = 2h, \tag{7}$$

und nach (5), (6):

$$\overset{\delta}{\Sigma}\overset{A}{\Sigma}(\delta, A) = 2^\nu g, \tag{8}$$

wenn g die Anzahl der Klassen des Hauptgeschlechtes (und folglich jedes Geschlechtes) bedeutet. Die Vergleichung gibt:

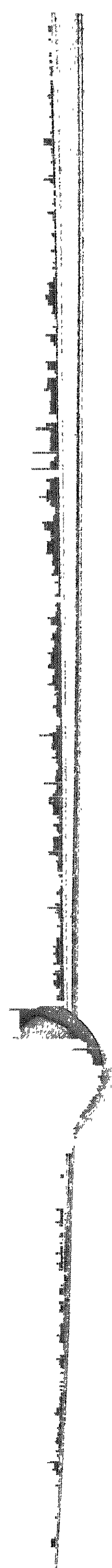
$$h = 2^{\nu-1} g, \tag{9}$$

also den Satz:

6. Die Anzahl der Geschlechter ist genau gleich $2^{\nu-1}$, d. h. gleich $\frac{1}{2}(Z, R)$, § 108, 9.

DRITTES BUCH.

KOMPLEXE MULTIPLIKATION.



Siebzehnter Abschnitt.

Elliptische Funktionen und quadratische Formen.

§ 114. Singuläre Perioden der doppelt periodischen Funktionen.

Bezeichnen wir mit $\varphi(u)$ eine doppelt periodische Funktion mit den Perioden ω_1, ω_2, so besitzt, wenn n eine ganze Zahl bedeutet, $\varphi(nu)$ dieselben Perioden, und hierauf beruht die Multiplikation der elliptischen Funktionen, die im sechsten Abschnitt betrachtet wurde. Es entsteht nun die Frage, ob sich nicht noch auf andere Weise ein Multiplikator μ so bestimmen läßt, daß $\varphi(\mu u)$ die Perioden ω_1, ω_2 besitzt, ob also eine Multiplikation auch mit nicht ganzzahligem Multiplikator existiert. Dies wird dann und nur dann der Fall sein, wenn für ein System ganzer Zahlen a, b, c, ∂ die Gleichungen bestehen:

$$\mu\omega_1 = a\omega_1 + b\omega_2,$$
$$\mu\omega_2 = c\omega_1 + \partial\omega_2.$$

Setzen wir, um die darin enthaltene Forderung näher zu ergründen:

$$\omega = \frac{\omega_2}{\omega_1}$$

und nehmen an, daß ω einen positiven imaginären Bestandteil habe, so folgt:

$$\mu = a + b\omega,$$

(1) $$\omega = \frac{c + \partial\omega}{a + b\omega}.$$

Solange ω als variabel betrachtet wird, ist diese Gleichung nur möglich, wenn $b = c = 0$, $a = \partial$ und μ also eine ganze Zahl ist.

Ist dagegen die Gleichung (1) nicht eine identische, so ist ω die Wurzel einer ganzzahligen quadratischen Gleichung:

$$b\omega^2 + (a - \partial)\omega - c = 0, \tag{2}$$

also, wenn wir

$$a\partial - bc = n$$
$$m = -4bc - (a - \partial)^2 = 4n - (a + \partial)^2$$

setzen, so ist

$$m \equiv 0 \quad \text{oder} \quad \equiv -1 \pmod 4,$$

und es ergibt sich:

$$\omega = \frac{-a + \partial + \sqrt{-m}}{2b},$$
$$\mu = \frac{a + \partial + \sqrt{-m}}{2},$$
$$n = \frac{a + \partial + \sqrt{-m}}{2} \cdot \frac{a + \partial - \sqrt{-m}}{2},$$
$$\mu^2 - (a + \partial)\mu + n = 0.$$

Damit ω einen positiven imaginären Teil habe, muß m und umsomehr also n positiv sein, und μ ist eine komplexe, ganze, algebraische Zahl. Daher erklärt sich die Bezeichnung komplexe Multiplikation.

Wenn nun umgekehrt ω einer quadratischen Gleichung

$$A\omega^2 + B\omega + C = 0 \tag{3}$$

genügt, worin A, B, C ganze Zahlen sind, und die Diskriminante

$$D = B^2 - 4AC \tag{4}$$

negativ ist, so ist ω nicht reell, und in einer der beiden Wurzeln von (3) ist der imaginäre Teil positiv. Diese soll für ω genommen werden. Es heißt dann ω eine Wurzel der quadratischen Form (A, B, C).

Unbeschadet der Allgemeinheit können A, B, C ohne gemeinsamen Teiler und A, C positiv angenommen werden. Es lassen sich dann für ω unendlich viele Relationen von der Form (1) [oder (2)] aufstellen. Man hat nur, wenn x eine ganze von Null verschiedene Zahl ist, zu setzen:

$$\begin{aligned} b &= Ax, \\ c &= -Cx, \\ a - \partial &= Bx. \end{aligned} \tag{5}$$

Setzt man noch

$$a + \delta = y, \tag{6}$$

so folgt:

$$\begin{aligned} a &= \frac{y + Bx}{2}, \\ b &= Ax, \\ c &= -Cx, \\ \delta &= \frac{y - Bx}{2}, \end{aligned} \tag{7}$$

woraus sich, wenn

$$a\delta - bc = n$$

gesetzt wird, ergibt:

$$4n = y^2 - Dx^2. \tag{8}$$

Die Zahl n wird also in die beiden komplexen ganzzahligen Faktoren

$$n = \frac{y + x\sqrt{D}}{2} \cdot \frac{y - x\sqrt{D}}{2}$$

zerlegt. Für ω und μ findet sich noch:

$$\omega = \frac{-B + \sqrt{D}}{2A} = \frac{2C}{-B - \sqrt{D}},$$

$$\mu = a + b\omega = \frac{y + \sqrt{D}x}{2}.$$

Die hier eingeführten Zahlen x, y sind nur an die eine Bedingung geknüpft, daß $y + Bx$ und folglich auch $y - Bx$ gerade Zahlen seien, damit a, δ nach (7) ganze Zahlen werden. Ist also B gerade, so muß y gerade sein, während x beliebig ist; ist B ungerade, so sind x und y beide gerade oder beide ungerade anzunehmen. Nach (4) kann man diese Unterscheidung auch so ausdrücken:

1) Ist $D \equiv 0 \pmod 4$, so ist $y \equiv 0 \pmod 2$,
2) Ist $D \equiv 1 \pmod 4$, so ist $y \equiv x \pmod 2$.

Sollen bei gegebenen A, B, C die Zahlen a, b, c, δ ohne gemeinsamen Teiler sein, so kommen noch andere Bedingungen hinzu:

Aus (5), (6) folgt, daß jeder gemeinsame Teiler von a, b, c, δ auch Teiler von x und y ist; umgekehrt ist jeder gemeinsame Teiler von x und y auch Teiler von b, c, $2a$, 2δ. Sollen also a, b, c, δ ohne gemeinsamen Teiler sein, so können x und y

keinen größeren gemeinsamen Teiler haben als 2. Haben x und y den größten gemeinschaftlichen Teiler 2, so sind b und c gerade und a, b, c, ∂ sind dann und nur dann relativ prim, wenn a und ∂, also auch $n = a\partial - bc$ ungerade sind.

Die Gleichung (8) hat, wenn wir von dem interesselosen Fall $n = 1$ absehen, keine diesen Bedingungen genügende Lösung, in der $x = 0$ ist. Ändern wir aber die Vorzeichen von x, y zugleich, so gehen a, b, c, ∂ nach (10) in $-a, -b, -c, -\partial$ über, und die Gleichung (1) ändert sich nicht. Die Transformation $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ bleibt also ungeändert.

Wir nennen jetzt der Kürze wegen eine Lösung der Gleichung (8) eine eigentliche Lösung und $n = \frac{1}{4}(y^2 - Dx^2)$ eine eigentliche Darstellung von n, wenn x und y den folgenden Bedingungen genügt:

x ist positiv.

Der größte gemeinschaftliche Teiler von x und y ist 1 oder 2.

Ist er $= 2$, so ist n ungerade.

Wenn nun ω einer gegebenen Gleichung (3) genügt, so ist durch jedes System $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ eine eigentliche Lösung von (8) eindeutig bestimmt. Denn nach (5) ist x der größte gemeinschaftliche Teiler von $b, c, a - \partial$, und durch (6) ist y bestimmt, und andererseits ist aus einer eigentlichen Lösung von (8) durch (7) das System a, b, c, ∂ vollständig bestimmt. Es ist aber noch die Frage zu entscheiden, ob zwei verschiedene eigentliche Lösungen x, y und x', y' zu äquivalentem System $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}, \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix}$ führen können. Unter äquivalentem System sind hier nach § 28, § 53 zwei solche zu verstehen, bei denen

$$(9) \qquad \begin{pmatrix} a', & b' \\ c', & \partial' \end{pmatrix} = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$$

ist, wenn $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ eine lineare Transformation ist, also

$$(10) \qquad \alpha\delta - \beta\gamma = 1.$$

Wenn wir beide Seiten der Gleichung (9) von rechts mit $\begin{pmatrix} \partial, & -b \\ -c, & a \end{pmatrix}$ zusammensetzen, so ergibt sich:

$$\begin{pmatrix} a'\partial - b'c, & -a'b + b'a \\ c'\partial - \partial'c, & -c'b + \partial'a \end{pmatrix} = \begin{pmatrix} n\alpha, & n\beta \\ n\gamma, & n\delta \end{pmatrix},$$

oder, wenn wir für a, b, c, ∂ die Ausdrücke (7) und für a', b', c', ∂' die entsprechenden

$$a' = \frac{y' + Bx'}{2}, \quad b' = Ax',$$
$$c' = -Cx', \quad \partial' = \frac{y' - Bx'}{2}$$

setzen:

$$\begin{pmatrix} \frac{yy' - Dxx' + B(x'y - y'x)}{4}, & A\frac{x'y - y'x}{2} \\ -C\frac{x'y - y'x}{2}, & \frac{yy' - Dxx' - B(x'y - y'x)}{4} \end{pmatrix} = \begin{pmatrix} n\alpha, & n\beta \\ n\gamma, & n\delta \end{pmatrix}.$$

Daraus folgt:

$$\begin{aligned} 4n\alpha &= yy' - Dxx' + B(x'y - y'x), \\ 2n\beta &= A(x'y - y'x), \\ 2n\gamma &= -C(x'y - y'x), \\ 4n\delta &= yy' - Dxx' - B(x'y - y'x), \\ \hline 2n(\alpha - \delta) &= B(x'y - y'x), \\ 2n(\alpha + \delta) &= yy' - Dxx'. \end{aligned}$$

Da nun A, B, C ohne gemeinsamen Teiler sind, so folgt, daß $x'y - y'x$ durch $2n$ teilbar sein muß, und nach der letzten Gleichung ist auch $yy' - Dxx'$ durch $2n$ teilbar. Also setzen wir

(11) $$\begin{aligned} x'y - y'x &= 2n\xi, \\ yy' - Dxx' &= 2n\eta \end{aligned}$$

und erhalten:

$$\alpha = \frac{\eta + B\xi}{2}, \quad \beta = A\xi,$$
$$\gamma = -C\xi, \quad \delta = \frac{\eta - B\xi}{2},$$

woraus nach (10) folgt:

(12) $$\eta^2 - D\xi^2 = 4.$$

Lösen wir die Gleichungen (11) nach x' und y' auf, so folgt:

(13) $$\begin{aligned} 2x' &= \xi y + \eta x, \\ 2y' &= \eta y + D\xi x. \end{aligned}$$

Ist $-D > 4$, so hat (12) nur die beiden Lösungen

(14) $$\xi = 0, \quad \eta = \pm 2,$$

und daraus ergibt sich, da x und x' positiv sein sollen:

$$x' = x, \qquad y' = y, \qquad (\eta = +2).$$

Ist aber $-D = 4$, so hat (12) außerdem noch die Lösung

$$\xi = \pm 1, \qquad \eta = 0,$$

und es folgt aus (13):

$$y' = \mp 2x,$$
$$x' = \pm \frac{y}{2},$$

und das Zeichen von η ist so zu bestimmen, daß x' positiv wird.

Ist endlich $-D = 3$, so haben wir außer (14) die Lösungen

$$\xi = \pm 1, \qquad \eta = \pm 1,$$

worin zunächst beide Zeichen beliebig sind.

Dann folgt aber aus (13):

$$\pm 2x' = x \pm y,$$
$$\pm 2y' = y \mp 3x,$$

und man kann die Vorzeichen auf zwei Arten so wählen, daß x' positiv wird. Wir haben also den Satz:

I. Bei gegebener Gleichung (3) führt jede eigentliche Lösung der Gleichung (8) zu einer Transformation $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ von der $n$ten Ordnung. Verschiedene Lösungen von (8) führen im allgemeinen zu nicht äquivalenten Systemen $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$. In den beiden Ausnahmefällen $D = -4$ und $D = -3$ führen je zwei oder je drei verschiedene Lösungen von (8) zu äquivalenten Systemen.

Bezeichnen wir mit k eine Zahl, die im allgemeinen gleich der Zahl der eigentlichen Lösungen von (8) ist, für $D = -4$ und $D = -3$ aber die Hälfte oder ein Drittel der Zahl dieser Lösungen, so können wir das Theorem I. so fassen:

II. Aus einer Gleichung (3) können wir k nicht äquivalente Systeme $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ ableiten, die der Gleichung (1) genügen.

§ 115. Die singulären Werte der Invariante $j(\omega)$.

Die Frage, die zunächst unser Interesse in Anspruch nimmt, ist die nach den Werten der Modulfunktionen von ω für die

besonderen Werte des Arguments ω, die wir im vorigen Paragraphen betrachtet haben. Von diesen hängen die Moduln der elliptischen Funktionen ab, die eine komplexe Multiplikation zulassen. Sie heißen nach Kronecker singuläre Moduln. Wir werden dementsprechend auch von den singulären Werten der Modulfunktionen, insbesondere von den singulären Invarianten $j(\omega)$ sprechen, und verstehen darunter die Werte, die diese Funktionen annehmen, wenn ω die Wurzel (mit positiv imaginärem Bestandteil) einer quadratischen Form mit negativer Diskriminante ist.

Wenn ω der Gleichung (3), § 114, genügt und a, b, c, ∂, n wie im vorigen Paragraphen bestimmt sind, so folgt zunächst:

$$j(\omega) = j\left(\frac{c + \partial\omega}{a + b\omega}\right), \tag{1}$$

und wenn also

$$F_n(u, v) = 0 \tag{2}$$

die zum Transformationsgrad n gehörige Invariantengleichung ist (§ 69), so ist (2) befriedigt, wenn a, b, c, ∂ ohne gemeinsamen Teiler sind und

$$u = j(\omega), \quad v = j\left(\frac{c + \partial\omega}{a + b\omega}\right) = u \tag{3}$$

gesetzt wird. Danach gelangen wir zu dem ersten Hauptsatz dieser Theorie:

III. Der singuläre Wert

$$u = j(\omega)$$

ist eine Wurzel der algebraischen Gleichung:

$$F_n(u, u) = 0. \tag{4}$$

Ist umgekehrt u eine Wurzel der Gleichung (4), so ist, wenn ω aus der Gleichung $j(\omega) = u$ bestimmt wird, einer von den der Gleichung (2) genügenden Werten von v gleichfalls $= u$, und es besteht also eine Gleichung von der Form (1); diese hat nach § 53 zur Folge, daß ω mit $\dfrac{c + \partial\omega}{a + b\omega}$ äquivalent ist, und daraus ergibt sich eine Gleichung von der Form § 114, (3). Also haben wir die Ergänzung zu III.:

IV. Jede Wurzel von (4) ist eine singuläre Invariante.

Ist τ eine Variable mit positiv imaginärem Teil, und v gleichfalls eine Variable, so zerfällt $F_n[v, j(\tau)]$ nach § 69 in die linearen Faktoren

$$v - j\left(\frac{c + \partial\tau}{a + b\tau}\right),$$

worin $\begin{pmatrix} a, & b \\ c, & \partial \end{pmatrix}$ ein vollständiges Repräsentantensystem nicht äquivalenter Transformationen $n$ten Grades durchläuft, und folglich kann $F_n(u, u)$ in die Faktoren

$$(5) \qquad j(\tau) - j\left(\frac{c + \partial\tau}{a + b\tau}\right)$$

zerlegt werden, wenn $u = j(\tau)$ gesetzt wird.

Aus dem Theorem II., § 114, aber folgt, daß, wenn wir $\tau = \omega$ setzen, k von den Faktoren (5) verschwinden. Wir können aber auch noch folgern, daß der Quotient

$$(6) \qquad \frac{j(\tau) - j\left(\frac{c + \partial\tau}{a + b\tau}\right)}{j(\tau) - j(\omega)}$$

für $j(\tau) = j(\omega)$ endlich und von Null verschieden bleibt. Denn differentiiert man Zähler und Nenner nach τ und setzt dann $\tau = \omega$, so ergibt sich der Grenzwert:

$$1 - \frac{n}{(a + b\omega)^2} = \frac{2\sqrt{D}x}{y + \sqrt{D}x},$$

der von Null verschieden ist.

Die Invariante $j(\omega)$ bleibt unverändert, wenn ω durch eine äquivalente Zahl ersetzt wird, hat aber für jede andere Zahl ω einen anderen Wert. Sie gehört also nicht zu der individuellen Form (A, B, C), sondern zu der ganzen Klasse äquivalenter Formen, und wird darum die Klasseninvariante genannt.

Ferner ist die Zahl k nicht von den Koeffizienten A, B, C, sondern nur von D und n abhängig, und ist daher für alle primitiven Formen der Diskriminante D dieselbe. Wir führen nun die folgende Funktion der Variablen u ein: Es bedeute $\omega_1, \omega_2, \ldots, \omega_h$ ein vollständiges System nicht äquivalenter Zahlen der Diskriminante D, also das System der Wurzeln eines Systems nicht äquivalenter Formen (A, B, C) der Diskriminante D. Wir setzen

$$(7) \qquad H_m(u) = [u - j(\omega_1)]\,[u - j(\omega_2)]\,\ldots\,[u - j(\omega_h)],$$

worin, wie wir jetzt öfter tun werden,

(8) $$m = -D$$

gesetzt ist, so daß m eine positive ganze Zahl bedeutet.

Diese Funktion, die für die Folge sehr wichtig ist, heißt die Klassenfunktion. Die Wurzeln der Gleichung

(9) $$H_m(u) = 0$$

sind die Klasseninvarianten der Diskriminante $D = -m$, und diese Gleichung heißt darum die Klassengleichung.

Der Grad h der Klassengleichung ist gleich der Zahl primitiver Klassen der quadratischen Formen der Diskriminante D. Wenn man nun die Quotienten (6) betrachtet, so ergibt sich aus alledem:

V. Die Funktion $F_n(u, u)$ ist durch $[H_m(u)]^k$ teilbar, und der Quotient ist relativ prim zu $H_m(u)$.

Hiernach läßt sich die Funktion $F_n(u, u)$ in Faktoren zerlegen, und es ergibt sich, wenn C eine Konstante ist, die gleich den Koeffizienten der höchsten Potenz u^N von u ist:

(10) $$F_n(u, u) = C H_m^k(u) H_{m'}^{k'}(u) H_{m''}^{k''}(u) \dots,$$

wenn sich das Produkt auf alle die positiven ganzen Zahlen m, m', m'', ... erstreckt, für die Gleichung § 114, (8)

(11) $$4n = y^2 + m x^2$$

eigentliche Lösungen zuläßt, und k, k', k'', ... jedesmal die Anzahl dieser Lösungen bedeutet (mit der dort angegebenen Modifikation in den beiden Ausnahmefällen $D = -4$, $D = -3$).

Es ist zunächst der Grad N der Gleichung $F_n(u, u)$ zu bestimmen.

Wenn wir die Repräsentanten in (5) wie in § 69 auswählen, so wird

(12) $$F_n[j(\tau), j(\tau)] = \Pi\left[j(\tau) - j\left(\frac{c + \partial\tau}{a}\right)\right].$$

Hierin bedeutete a, ∂ alle der Bedingung $a\partial = n$ genügenden Paare positiver ganzer Zahlen, und c durchläuft ein Restsystem nach dem Modul a, mit Ausschluß solcher Werte, die zu dem größten gemeinschaftlichen Teiler e von a und ∂ nicht relativ prim sind, so daß die Anzahl der Werte von c, die zu einer Zerlegung von n in die beiden Faktoren a und ∂ gehören, gleich $a\varphi(e):e$ ist. Ist nun N der Grad von $F_n(u, u)$ und C der Koeffizient der höchsten Potenz von u, so beginnt die Entwickelung

von $F_n[j(\tau), j(\tau)]$ nach Potenzen von $q = e^{\pi i \tau}$ mit $C q^{-2N}$ [§ 69, (4)].

Wenn wir also die Faktoren der rechten Seite von (12) in gleicher Weise entwickeln, so können wir sowohl C als N bestimmen.

Für einen Faktor der rechten Seite von (1)

$$j(\tau) - j\left(\frac{c + \partial\tau}{a}\right)$$

haben wir folgende Anfänge der Entwickelung

$$\begin{array}{lll} 1. & -q^{-\frac{2\partial}{a}} e^{-\frac{2\pi i c}{a}}, & \partial > a, \\ 2. & q^{-2}, & \partial < a, \\ 3. & q^{-2}\left(1 - e^{-\frac{2\pi i c}{a}}\right), & \partial = a. \end{array}$$

Nehmen wir zunächst an, n sei kein Quadrat, so kommt der Fall 3. nicht vor, und es ist

$$N = \sum_{\partial > a} \frac{\partial}{e}\, \varphi(e) + \sum_{\partial < a} \frac{a}{e}\, \varphi(e),$$

oder, was dasselbe ist,

$$N = 2 \sum_{\partial > a} \frac{\partial}{e}\, \varphi(e). \tag{13}$$

C ist nach 1. jedenfalls eine $n$te Einheitswurzel, und da es zugleich eine rationale Zahl ist, so muß es $= \pm 1$ sein.

Ist sodann n ein Quadrat, so kommen $\varphi(\sqrt{n})$ Faktoren von der Form 3. vor und es ergibt sich:

$$N = 2 \sum_{\partial > a} \frac{\partial}{e}\, \varphi(e) + \varphi(\sqrt{n}). \tag{14}$$

C ist hier zwar auch von Null verschieden, aber nicht gleich ± 1. Den Wert von C brauchen wir in diesem Falle nicht näher zu bestimmen. (Er ist, wie aus der Kreisteilungstheorie folgt, immer ein Teiler von $\sqrt{n}$).

Wenn im besondern n eine Primzahl ist, so ist

$$N = 2n. \tag{15}$$

Man kann über x und y immer so verfügen, daß unter Einhaltung der Bedingungen § 114 $n = \frac{1}{4}(y^2 + m x^2)$ kein Quadrat wird. Zu dem Ende nehme man x durch 4, y durch 2, aber nicht durch 4 teilbar, und überdies y ohne ungeraden gemeinsamen Teiler mit $m x^2$ an. Ist dann $\frac{1}{4}(y^2 + m x^2)$ ein Quadrat M^2, so

hat es einen ungraden quadratischen Primteiler p^2, der nicht in y^2 aufgeht, und es ist

$$(y + 4\lambda p)^2 + m x^2 = 4 M^2 + 8\lambda y p + 16\lambda^2 p^2,$$

und diese Zahl ist, wenn λ nicht durch p teilbar ist, zwar durch p, aber nicht durch p^2 teilbar, und kann also kein Quadrat sein. Überdies kann man über λ noch so verfügen, daß $y + 4\lambda p$ mit x keinen ungeraden gemeinsamen Teiler hat, daß also die Bedingungen § 114 erfüllt sind. Demnach genügt $j(\omega)$ für jedes m einer Gleichung $F_n(u, u)$, in der $C = \pm 1$ ist, und daraus folgt nach Bd. II, § 149:

VI. Die Klassenvarianten sind ganze algebraische Zahlen.

§ 116. Klassenzahlrelationen.

Wenn man den Grad, wie er sich hiernach für beide Teile der Gleichung (10), § 115 ergibt, gleich setzt, so erhält man die Formel

$$N = hk + h'k' + h''k'' + \cdots, \tag{1}$$

$$\Sigma hk = 2\Sigma \frac{\partial}{e}\varphi(e) + \varphi(\sqrt{n}), \tag{2}$$

worin $\varphi(\sqrt{n}) = 0$ zu setzen ist, wenn n kein Quadrat ist, und N durch (13), (14) oder (15) des vorigen Paragraphen bestimmt ist. Dies ist die Kroneckersche Klassenzahlrelation, der wir noch eine etwas bequemere Form geben wollen [1]).

Wir fassen neben n alle Werte n' ins Auge, die aus n durch Fortheben eines quadratischen Faktors entstehen, bilden für sie die Gleichung (2) und addieren alle so gewonnenen Resultate. Dabei ist nur, falls n ein Quadrat ist, der Wert $n' = 1$ auszuschließen, weil $F_1(u, u) = 0$ ist.

Es sei also δ^2 irgend ein von n selbst verschiedener quadratischer Faktor von n und

$$n = n'\delta^2.$$

Zerlegen wir n' in zwei Faktoren $n' = a'\partial'$ und bezeichnen mit e' den größten gemeinschaftlichen Teiler von ∂' und a', so ist

[1]) Die Klassenzahlrelationen, von denen die hier abgeleitete nur der einfachste Fall ist, sind von Kronecker entdeckt (Crelles Journal, Bd. 57) und von Gierster (Mathematische Annalen, Bd. 21, 22) und Hurwitz (ebenda Bd. 25) bedeutend verallgemeinert.

(3) $$\Sigma N' = 2\sum^{\delta}\sum_{\partial' > a'}^{\partial'} \frac{\partial'}{e'}\varphi(e') + \sum^{n'}\varphi(\sqrt{n'}),$$

wenn δ^2 alle quadratischen Faktoren von n (mit etwaiger Ausnahme von n selbst) durchläuft.

Setzen wir nun

$$\partial'\delta = \partial, \quad a'\delta = a, \quad e'\delta = e,$$

so ist $a\partial = n$, und e ist der größte gemeinschaftliche Teiler von a und ∂; zugleich hat $\partial' > a'$ zur Folge, daß $\partial > a$ ist. Umgekehrt erhält man aus jeder Zerlegung $a\partial$ von n und jedem Teiler e' von e eine Zerlegung $a'\partial'$ von n', wobei

$$\delta = \frac{e}{e'}, \quad \partial' = \frac{\partial e'}{e}, \quad a' = \frac{a e'}{e}$$

wird. Demnach ist

(4) $$\Sigma N' = 2\sum_{\partial > a} \frac{\partial}{e} \Sigma\varphi(e') + \sum^{n'}\varphi(\sqrt{n'}).$$

Hierin machen wir nun Gebrauch von der zahlentheoretischen Relation: $\Sigma\varphi(\partial) = n$, worin sich die Summe auf alle Divisoren von n bezieht. Nehmen wir zunächst an, daß n kein Quadrat sei, so sind auch alle n' keine Quadrate und $\varphi(\sqrt{n'}) = 0$. Also erhalten wir wegen $\Sigma\varphi(e') = e$

(5) $$\Sigma N' = 2\sum_{\partial > \sqrt{n}} \partial.$$

Wenn dagegen n ein Quadrat ist, so durchläuft e' noch immer die sämtlichen Divisoren von e, $\sqrt{n'}$ aber die sämtlichen Divisoren von $\sqrt{n}$, mit Ausnahme von 1; danach ergibt sich für diesen Fall:

(6) $$\Sigma N' = 2\sum_{\partial > \sqrt{n}} \partial + \sqrt{n} - 1.$$

In beiden Fällen durchläuft ∂ die sämtlichen Divisoren von n, die größer als $\sqrt{n}$ sind.

Wir haben nun noch die Summe der Ausdrücke $\Sigma k h$ für die verschiedenen Werte von n' oder δ zu bilden. Setzen wir aber $n = \delta^2 n'$, so erhalten wir aus jeder eigentlichen Lösung von

(7) $$4n' = y'^2 + m x'^2$$

durch Multiplikation mit δ^2 eine (wenn $\delta > 1$ ist, uneigentliche) Lösung von

(8) $$4n = y^2 + m x^2,$$

nämlich

$$y = \delta y', \quad x = \delta x'.$$

Ist umgekehrt irgend eine Lösung x, y von (8) gegeben, so ist $4n$ durch das Quadrat eines jeden gemeinschaftlichen Teilers von x und y teilbar. Wir bezeichnen mit δ den größten gemeinschaftlichen Teiler von x, y, dessen Quadrat zugleich Teiler von n ist, der also entweder gleich dem größten gemeinschaftlichen Teiler von x, y oder gleich der Hälfte desselben ist, und setzen

$$y = \delta y', \quad n = \delta x',$$

und erhalten so eine eigentliche Lösung von (7).

Wenn wir also für $-m$ alle Diskriminanten setzen, für die die Gleichung (8) überhaupt Lösungen hat, und mit k die Anzahl dieser Lösungen (mit positivem x) verstehen, ferner mit $h(m)$ die Klassenzahl primitiver Formen der Diskriminante $-m$, so ergibt sich die Formel

$$(9) \qquad \Sigma k h(m) = 2 \Sigma \partial,$$

wenn n kein Quadrat ist,

$$= 2 \Sigma \partial + \sqrt{n} - 1,$$

wenn n ein Quadrat ist.

Hier ist noch daran zu erinnern, daß in den beiden Ausnahmefällen $m = 3$, $m = 4$ unter k in § 115 nur der dritte Teil oder die Hälfte der Zahl der eigentlichen Lösungen von (8) verstanden war.

Diesem Umstand wollen wir jetzt dadurch gerecht werden, daß wir unter k die Gesamtzahl der Lösungen von (8) verstehen, aber

$$h(3) = \tfrac{1}{3}, \quad h(4) = \tfrac{1}{2}$$

setzen [statt $h(3) = 1$, $h(4) = 1$].

Es ist ferner zu bemerken, daß bei der Bildung der Summe (9) die zu dem Wert $n' = 1$ gehörigen Lösungen nicht mitgezählt sind. Dies kommt nur für den Fall in Betracht, daß n ein Quadrat ist. Es hat dann die Gleichung (7):

$$4 = y'^2 + m x'^2$$

nur die folgenden eigentlichen Lösungen:

$$\begin{aligned} m = 3:\ & x' = 1, \quad y' = \pm 1, \quad k = 2, \quad h = \tfrac{1}{3}, \\ m = 4:\ & x' = 1, \quad y' = 0, \quad\ \ k = 1, \quad h = \tfrac{1}{2}, \end{aligned}$$

und es würde also, wenn man diese Ausnahme beseitigen wollte, zu (9) noch zu addieren sein:

$$\Sigma k h, \text{ auf } n' = 1 \text{ bezogen}, = \tfrac{1}{2} + \tfrac{2}{3} = \tfrac{7}{6}.$$

Demnach lautet jetzt die Formel

(10) $$\Sigma k\, h(m) = 2\,\Sigma\,\partial,$$

n kein Quadrat,

$$= 2\,\Sigma\,\partial + \sqrt{n} + \tfrac{1}{6},$$

n ein Quadrat.

Die Summe auf der linken Seite von (10) zerlegen wir in ihre einzelnen Bestandteile, indem wir jede Lösung der Gleichung (8) besonders nehmen. Dann bekommen wir eine Summe von Ausdrücken $h(m)$, wo aber dasselbe m so oft vorkommt, als (8) Lösungen hat. Eine der Lösungen ergibt aber

$$m = \frac{4n - y^2}{x^2},$$

und diese kommt, wenn $y = 0$ ist, einmal, wenn y von Null verschieden ist, zweimal (mit $+y$ und $-y$) vor. Es ist aber die Anzahl der primitiven Klassen der Diskriminante $-m$ gleich der Anzahl der nicht primitiven Klassen der Diskriminante $-x^2 m$ vom Teiler x, und wenn wir also jetzt (zum Unterschied von der vorigen Formel) mit $h(m)$ die Gesamtzahl der Klassen von der Diskriminante $-m$ (primitiven und imprimitiven) verstehen, so erhalten wir aus (10):

(11) $$h(4n) + 2h(4n-1) + 2h(4n-4) + 2h(4n-9) + \cdots$$

$$= 2\sum_{\partial > \sqrt{n}} \partial, \qquad (n \text{ kein Quadrat}),$$

$$= 2\sum_{\partial > \sqrt{n}} \partial + \sqrt{n} + \tfrac{1}{6}, \qquad (n \text{ ein Quadrat}).$$

Darin ist links die Summe der $h(4n - y^2)$ so lange fortzusetzen, als $4n - y^2$ positiv bleibt, und rechts durchläuft ∂ alle Divisoren von n, die größer als $\sqrt{n}$ sind.

Dabei ist jedoch zu beachten, daß die Formen $(x, 0, x)$ nur je mit $\frac{1}{2}$ und (x, x, x) mit $\frac{1}{3}$ in Rechnung zu setzen sind, weil sie aus den Darstellungen von $4n$ durch die Diskriminante $m = -4, -3$ hervorgehen.

§ 117. Arithmetische Natur der Klassenfunktion $H_m(u)$.

Wir kehren jetzt wieder zurück zu der Gleichung (10), § 115, um daraus die Natur der Koeffizienten der Klassengleichung $H_m(u) = 0$ abzuleiten. Zunächst aber betrachten wir die beiden speziellen Fälle: $m = 4$ und $m = 3$.

Setzen wir wie in § 54, (4)

$$\gamma_2(\omega) = \sqrt[3]{j(\omega)}, \quad \gamma_3(\omega) = \sqrt[2]{j(\omega) - 1728},$$

so ergibt sich aus § 54, (14):

$$\gamma_3(i) = -\gamma_3(i), \quad \text{also} \quad \gamma_3(i) = 0.$$

Es ist ferner nach derselben Formel, wenn wir

$$\varrho = \frac{-1 + i\sqrt{3}}{2}, \qquad \varrho + 1 = \frac{-1}{\varrho}$$

setzen:

$$\gamma_2(\varrho + 1) = e^{-\frac{2\pi i}{3}} \gamma_2(\varrho) = \gamma_2\left(-\frac{1}{\varrho}\right) = \gamma_2(\varrho),$$

folglich $\gamma_2(\varrho) = 0$, und wir erhalten

$$(1) \qquad \begin{aligned} H_3(u) &= u, & j(\varrho) &= 0, \\ H_4(u) &= u - 1728, & j(i) &= 1728. \end{aligned}$$

Es haben also die beiden Funktionen $H_3(u)$ und $H_4(u)$ ganze rationale Zahlenkoeffizienten. Diese Eigenschaft können wir nun durch vollständige Induktion allgemein für alle H_m nachweisen.

Zunächst bemerken wir, daß, wenn bewiesen ist, daß $H_m(u)$ rationale Koeffizienten hat, sogleich folgt, daß die Koeffizienten ganze rationale Zahlen sind (der erste $= 1$). Denn diese Koeffizienten sind ganze algebraische Zahlen (nach § 115, VI.) und folglich, wenn sie rational sind, ganze rationale Zahlen. Nun betrachten wir die größten unter den Werten von m, die in der Gleichung (10), § 115 vorkommen; das sind

$$\begin{aligned} m &= 4n, & x &= 1, & y &= 0, & k &= 1, \\ m &= 4n - 1, & x &= 1, & y &= \pm 1, & k &= 2. \end{aligned}$$

Es enthält hiernach $F_k(u, u)$ die beiden Faktoren $H_{4n}(u)$, $H_{4n-1}(u)^2$, und sonst lauter Faktoren $H_m(u)$, in denen $m < 4n - 1$ ist. Nehmen wir an, daß von den letzteren schon bewiesen sei, daß sie rationale Koeffizienten haben, so folgt, daß

$$H_{4n}(u) H_{4n-1}(u)^2 = \Phi(u)$$

rationale Koeffizienten hat, und man hat also, um $H_{4n-1}(u)$ zu finden, den größten gemeinschaftlichen Teiler von $\Phi(u)$ und $\Phi'(u)$ zu suchen, was durch rationale Rechnung geschieht. Damit ist aber auch $H_{4n}(u)$ auf rationalem Wege gefunden, und da $H_3(u)$ und $H_4(u)$ rationale Koeffizienten haben, so folgt allgemein:

VII. Die Klassenfunktionen $H_m(u)$ haben ganze rationale Zahlenkoeffizienten.

§ 118. Komposition der quadratischen Formen.

Da wir uns in der algebraischen Theorie der Klassengleichung auf die Theorie der Komposition der quadratischen Formen stützen müssen, so schicken wir darüber die folgenden Bemerkungen voraus:

Zwei primitive Formen $\varphi_1 = (a_1, b_1, c_1)$, $\varphi_2 = (a_2, b_2, c_2)$ der Diskriminante $-m$ heißen einhellig (einig, concordantes), wenn $a_1, a_2, \frac{1}{2}(b_1 + b_2)$ ohne gemeinschaftlichen Teiler sind; φ_1 und φ_2 sind also gewiß einhellig, wenn schon a_1, a_2 ohne gemeinsamen Teiler sind, und da man, wenn nur die Klassen k_1, k_2 von φ_1, φ_2 gegeben sind, φ_1, φ_2 in ihren Klassen immer so wählen kann, so folgt, daß man in irgend zwei Klassen (die auch identisch sein können), immer zwei einhellige Formen finden kann. Wenn also diese Voraussetzung zutrifft, so folgt aus

$$\tfrac{1}{4}(b_1^2 - b_2^2) = \tfrac{1}{2}(b_1 - b_2) \cdot \tfrac{1}{2}(b_1 + b_2) = a_1 c_1 - a_2 c_2,$$

daß $\frac{1}{2}(b_1 - b_2)$ durch den größten gemeinschaftlichen Teiler δ von a_1, a_2 teilbar ist, und daraus, daß man die beiden Kongruenzen

$$(1) \qquad b' \equiv b_1 \pmod{2 a_1}, \quad b' \equiv b_2 \pmod{2 a_2}$$

immer befriedigen kann.

Denn aus der ersten von ihnen folgt $b' = b_1 + 2 \lambda a_1$, und man hat also λ aus der Kongruenz

$$\tfrac{1}{2}(b_1 - b_2) + a_1 \lambda \equiv 0 \pmod{a_2}$$

zu bestimmen, die immer lösbar ist. Ist μ das kleinste gemeinschaftliche Vielfache von a_1 und a_2, also $a_1 a_2 = \mu \delta$, so kann b' nach (1) noch durch $b = b' + 2 \mu h$ ersetzt werden, wenn h eine beliebige ganze Zahl ist. Da nun $\frac{1}{4}(b_1^2 + m)$ durch a_1, $\frac{1}{2}(b_2^2 + m)$ durch a_2 teilbar ist, so ist $\frac{1}{4}(b'^2 + m)$ durch μ teilbar, und wenn wir h aus der Kongruenz

$$\frac{b'^2 + m}{4 \mu} + b' h \equiv 0 \pmod{\delta}$$

bestimmen, die immer lösbar ist, da b' nach Voraussetzung relativ prim zu δ ist, so wird $b^2 + m = 4 a_1 a_2 c$ durch $4 a_1 a_2$ teilbar. Die zwei Klassen k_1, k_2 sind dann repräsentiert durch

$$\varphi_1 = (a_1, b, a_2 c), \quad \varphi_2 = (a_2, b, a_1 c),$$

und die Form

$$\varphi = \varphi_1 \varphi_2 = (a_1 a_2, b, c)$$

ist aus $\varphi_1 \varphi_2$ komponiert. Die Form φ gehört in eine Klasse k, die aus k_1, k_2 komponiert heißt.

Nehmen wir $\varphi = (a, b, c)$ so an, daß a relativ prim zu m ist, so ist auch b relativ prim zu a (wegen $m = 4ac - b^2$). Ist $a = a_1 a_2$, so sind auch $(a_1, b, c a_2)$, $(a_2, b, c a_1)$ einhellige primitive Formen, und man erhält die Komposition

$$(a, b, c) = (a_1, b, c a_2), (a_2, b, c a),$$

und durch wiederholte Anwendung dieses Satzes gelangt man zu dem Resultat:

I. Die Form $\varphi = (a, b, c)$ läßt sich, wenn a relativ prim zu m ist, aus solchen Formen zusammensetzen, deren erste Koeffizienten Primzahlen, nämlich die Primfaktoren von a sind.

Eine dieser Komponenten, etwa

$$(p, b, a c p^{-1}),$$

läßt sich durch eine äquivalente Form $(p, b', c' p^g)$ ersetzen, deren dritter Koeffizient $c' p^g$ durch eine beliebig hohe Potenz von p teilbar ist.

Um dies zu beweisen, brauchen wir für die Äquivalenz das Zeichen $\sim$, und haben

$$(p, b, c p^{g-1}) \sim (p, b + 2\lambda p^g, c' p^g),$$

worin c' wegen der Gleichheit der Diskriminanten aus

$$p c' = c + \lambda b + \lambda^2 p^g$$

zu bestimmen ist. Da nun b durch p nicht teilbar ist, so kann λ aus der Kongruenz $c + \lambda b \equiv 0 \pmod{p}$ bestimmt werden, und c' ergibt sich als ganze Zahl. Damit ist mit Rücksicht auf (I.) bewiesen:

II. Man kann in jeder Klasse k von primitiven Formen der Diskriminante D einen Repräsentanten φ finden, der sich aus Formen

$$P = (p, b, p^g c),$$

worin p eine in D nicht aufgehende Primzahl, und g ein beliebiger Exponent ist, zusammensetzen läßt.

Die Form P läßt sich leicht mit sich selbst zusammensetzen, denn es ist im Sinne der Kompositionen, wenn $g > \nu$ ist:

$$(p^\nu, b, p^{g-\nu} c)(p, b, p^g c) = (p^{\nu+1}, b, p^{g-\nu-1} c),$$

und folglich durch den Schluß von $\nu - 1$ auf ν:

$$(2) \qquad P^\nu = (p^\nu, b, p^{g-\nu} c).$$

In der Kette der Kompositionen

(3) $$P, P^2, P^3, \ldots$$

kann eine Form vorkommen, die in die Hauptklasse gehört, die also mit $(1, 0, \frac{1}{4}m)$ oder $[1, 1, \frac{1}{4}(m+1)]$ äquivalent ist. Wenn dies bei P^ε eintritt, so ist p^ε durch die Hauptform darstellbar, und es gibt eine eigentliche Darstellung

(4) $$4p^\varepsilon = y^2 - Dx^2.$$

Ist umgekehrt eine solche Darstellung möglich, so gibt es in der Hauptklasse eine Form (p^ε, b, c).

Ist ε der kleinste positive Exponent, für den die Gleichung (4) eigentlich lösbar ist, so heißt ε der Index von p, und p gehört zum Exponenten ε.

Ist

(5) $$P = (p, b, p^{\varepsilon-1}c),$$

so ist

$$b^2 \equiv D \pmod{4p^\varepsilon},$$

und wenn diese Bedingung erfüllt ist, so ist in der Form (p, b, c') der Diskriminante D der dritte Koeffizient durch $p^{\varepsilon-1}$ teilbar. Die Form (5) bleibt erhalten, wenn wir b durch irgend eine nach dem Modul $2p^\varepsilon$ kongruente Zahl b' ersetzen. Ist also a nicht durch p teilbar und

$$\varphi = (a, B, C)$$

irgend eine mit P einhellige Form der Diskriminante D, so lassen sich die beiden Kongruenzen

$$x \equiv b \pmod{2p^\varepsilon}, \quad x \equiv B \pmod{2a}$$

zugleich befriedigen, und wenn man dieses x also an Stelle von b und B setzt, folgt:

III. Ist l die Klasse von P und k eine beliebige Klasse der Diskriminante D, so kann man in l und k die Repräsentanten wählen:

(6) $$(p, b, acp^{\varepsilon-1}), \quad (a, b, cp^\varepsilon),$$

und in der komponierten Klasse lk erhält man einen Repräsentanten

(7) $$(ap, b, p^{\varepsilon-1}c).$$

Ist also

$$\omega = \frac{-b+\sqrt{-m}}{2a}$$

eine Wurzel der Klasse k, so ist $\omega : p$ eine Wurzel der Klasse lk.

§ 119. Die Diskriminante der Invariantengleichung.

Wir stellen uns jetzt die Frage, wann eine Invariantengleichung

(1) $$F_p(v, u) = 0,$$

worin p eine Primzahl ist, für $u = j(\omega)$ zwei oder mehrere gleiche Wurzeln v hat, oder wann unter den $p + 1$ Größen

(2) $$j(p\,\omega),\quad j\left(\frac{\omega + c}{p}\right),\quad c = 0, 1, \ldots, p - 1$$

zwei oder mehrere einander gleiche vorkommen. Dies findet dann und nur dann statt, wenn unter den $p + 1$ Größen

(3) $$p\,\omega,\quad \frac{\omega + c}{p}$$

zwei äquivalente vorkommen. Es muß also jedenfalls ω einer ganzzahligen quadratischen Gleichung mit negativer Diskriminante $D = -m$ genügen, die wir in der Form annehmen:

(4) $$A\,\omega^2 + B\,\omega + C = 0,\quad 4\,A\,C - B^2 = m > 0,$$

worin A, B, C ohne gemeinsamen Teiler sind.

Ersetzen wir ω durch eine äquivalente Zahl, also (4) durch eine äquivalente Gleichung, so werden die Größen (2) nur untereinander vertauscht. Die Frage nach der Anzahl der gleichen Wurzeln von (1) wird also davon nicht berührt, und wir können daher annehmen, daß A durch p nicht teilbar sei. Ist nun zunächst $p\,\omega$ äquivalent mit $\frac{\omega + c}{p}$, so ist:

(5) $$\frac{\omega + c}{p} = \frac{\gamma + \delta\,p\,\omega}{\alpha + \beta\,p\,\omega},\quad \alpha\delta - \beta\gamma = 1.$$

Schreiben wir diese Gleichung so:

(6) $$\beta\,p\,\omega^2 + (\alpha + \beta\,c\,p - \delta\,p^2)\,\omega + c\,\alpha - \gamma\,p = 0,$$

so folgt durch Vergleichung mit (4) (da A durch p unteilbar sein sollte), daß α durch p teilbar, also $= p\,\alpha'$ sein muß, und daß eine ganze Zahl x existiert, die den Bedingungen genügt:

(7) $$\beta = A\,x,\quad \alpha' + \beta\,c - \delta\,p = B\,x,\quad c\,\alpha' - \gamma = C\,x.$$

Setzen wir noch

(8) $$\alpha' - \beta\,c + \delta\,p = y,$$

so folgt:

(9) $$\begin{aligned} 2\,\alpha' &= B\,x + y, \\ 2\,(\beta\,c - \delta\,p) &= B\,x - y, \end{aligned}$$

und aus

(10) $$p\alpha'\delta - \beta\gamma = 1$$

folgt sodann

(11) $$y^2 + m x^2 = 4.$$

Der Wert $x = 0$ ist auszuschließen, weil sonst $\beta = 0$ sein müßte, was der Gleichung (10) widerspricht, und wir können unbeschadet der Allgemeinheit x positiv annehmen. Da überdies m nach dem Modul 4 entweder $\equiv 0$ oder $\equiv 3$ sein muß, so bleiben zur Erfüllung von (11) nur folgende zwei Möglichkeiten übrig:

1. $$m = 3, \quad x = 1, \quad y = \pm 1.$$

Da es für die Diskriminante -3 nur eine Formenklasse gibt, so können wir $A = 1$, $B = 1$, $C = 1$ annehmen, d. h. für ω die imaginäre dritte Einheitswurzel $e^{\frac{2\pi i}{3}}$ setzen, und erhalten unter den Größen (3) drei äquivalente, indem wir $y = +1$ und $= -1$ annehmen:

(12) $$p\omega, \quad \frac{\omega}{p}, \quad \frac{\omega + 1}{p},$$

wie auch aus den Gleichungen

$$\frac{\omega}{p} = \frac{-1}{p + p\omega}, \quad \frac{\omega + 1}{p} = \frac{-1}{p\omega}$$

erkannt wird, aus denen die Äquivalenz der drei Größen (12) evident ist.

2. $$m = 4, \quad x = 1, \quad y = 0.$$

Weil es auch hier nur eine Formenklasse gibt, so können wir $B = 0$, $A = C = 1$, d. h. $\omega = i$ annehmen, und finden die zwei äquivalenten Werte:

$$p\omega, \quad \frac{\omega}{p},$$

wie auch aus der Gleichung

$$p\omega = \frac{-p}{\omega}$$

folgt.

Es seien ferner zwei der Werte (3)

$$\frac{\omega + c}{p}, \quad \frac{\omega + c'}{p}$$

äquivalent, so daß eine Gleichung besteht:

(13) $$\frac{\omega + c}{p} = \frac{\gamma p + \delta(\omega + c')}{\alpha p + \beta(\omega + c')}, \quad \alpha\delta - \beta\gamma = 1,$$

oder

(14) $$\beta\omega^2 + (\beta c' + \beta c + \alpha p - \delta p)\omega + \beta c c' + \alpha c p - \delta c' p - \gamma p^2 = 0,$$

woraus durch Vergleichung mit (4):

(15) $$\begin{aligned} \beta &= A x, \\ \beta c' + \beta c + \alpha p - \delta p &= B x, \\ \beta c c' + \alpha c p - \delta c' p - \gamma p^2 &= C x, \end{aligned}$$

und wenn man wieder

(16) $$\beta c' - \beta c + \alpha p + \delta p = y$$

setzt:

(17) $$\begin{aligned} 2(\beta c' + \alpha p) &= B x + y, \\ 2(\beta c - \delta p) &= B x - y. \end{aligned}$$

Daraus

(18) $$y^2 + m x^2 = 4 p^2.$$

Ist x durch p teilbar, so muß auch y durch p teilbar sein, und wir kommen durch Wegheben des Faktors p^2 auf die Gleichung (11) zurück, die, wie wir gesehen haben, nur für die Fälle $m = 3$ und $m = 4$ lösbar ist. Wir nehmen also weiter an, x sei durch p unteilbar.

Ist m durch p teilbar, so ist auch y durch p teilbar, β ist nach (15) nicht durch p teilbar. Dann aber folgt aus (16): $c \equiv c' \pmod{p}$, und beide entsprechen also der nämlichen Wurzel von (1).

Es gehe jetzt also p weder in x noch in m auf. Dann geht es auch nicht in y auf, und nach (17) werden c und c' aus den Kongruenzen

(19) $$\beta c' \equiv \frac{B x + y}{2}, \quad \beta c \equiv \frac{B x - y}{2} \pmod{p}$$

bestimmt, und wenn c, c' bestimmt sind, ergeben sich aus (17) α und δ als ganze Zahlen. Damit sind die beiden ersten Gleichungen (15) befriedigt, und γ erhält man aus der letzten Gleichung (15) gleichfalls als ganze Zahl.

Es ist nämlich

(20) $$\gamma p^2 = \beta c c' + (\alpha c - \delta c') p - C x \equiv 0 \pmod{p^2}.$$

Denn wir haben aus (17) und (15)

$$\begin{aligned} &\beta^2 c c' + \beta(\alpha c - \delta c')p - \alpha\delta p^2 - A C x^2 \\ &= \beta[\beta c c' + (\alpha c - \delta c')p - C x] - \alpha\delta p^2 \\ &= -\frac{y^2 + m x^2}{4} = -p^2; \end{aligned}$$

folglich ist das zweite Glied von (20) durch p^2 teilbar, und wenn man γp^2 dafür einsetzt, so folgt

$$\alpha\delta - \beta\gamma = 1.$$

Wir kommen also zu dem Resultat:

IV. Die Invariantengleichung $F_p(v, u)$ hat immer dann und nur dann mehrfache Wurzeln, wenn $u = j(\omega)$ ist, worin ω die Wurzel einer quadratischen Gleichung ist, deren Diskriminante nicht durch p teilbar ist, aber eine Lösung der Gleichung (18) gestattet.

Es gibt für ein gegebenes p nur eine endliche Anzahl von Werten m, die dieser Forderung entsprechen, da $m < 4p^2$ sein muß. Die Werte $m = 3$, $m = 4$ sind darunter als spezielle Fälle enthalten.

Da nach (18) $-m$ quadratischer Rest von p ist, so ist p durch eine Form der Diskriminante $-m$ darstellbar; p^2 ist aber durch die Hauptform einer Diskriminante darstellbar. Die Formenklasse, durch die p darstellbar ist, ist also selbst entweder die Hauptklasse oder sie gibt, mit sich selbst komponiert, die Hauptklasse, ist also zweiseitig. Wir können das Theorem IV. also auch folgendermaßen aussprechen:

V. Die Wurzeln der Diskriminante der Invariantengleichung $F_p(v, u)$ sind die singulären Invarianten $j(\omega)$, worin ω die Wurzel einer quadratischen Gleichung von negativer Diskriminante D ist, für die die Primzahl p den Index 1 oder 2 hat.

Achtzehnter Abschnitt.

Galoissche Gruppe der Klassengleichung.

---

§ 120. Relationen zwischen den Klasseninvarianten derselben Diskriminante.

Es ist für die Folge eine Bezeichnung zweckmäßig, durch die die Abhängigkeit der Klasseninvariante von der Formenklasse einfacher ausgedrückt wird. Wir setzen daher, wenn k eine beliebige primitive Klasse der Diskriminante $-m$ bedeutet, die nach § 118, III. durch $(a, b, c p^{\varepsilon})$ repräsentiert wird:

$$(k) = j\left(\frac{-b + \sqrt{-m}}{2a}\right) = j(\omega).$$

Wenn eine oder mehrere der (k) unter einem Funktionszeichen auftreten, so werden wir die Klammern auch weglassen, also z. B. $f(k, k', \ldots)$ für $f[(k), (k'), \ldots]$ schreiben.

Ist also

$$(1) \qquad (k) = j(\omega),$$

und l eine durch $(p, b, a c p^{\varepsilon - 1})$ repräsentierte Klasse, so ist nach § 118, III.:

$$(2) \qquad (l k) = j\left(\frac{\omega}{p}\right),$$

und es genügen also die beiden Größen

$$u = (k), \quad v = (l k)$$

der Invariantengleichung

$$(3) \qquad F_p(v, u) = 0.$$

Die Größe $v = (l k)$ ist aber außerdem eine Wurzel der Klassengleichung

$$(4) \qquad H_m(v) = 0,$$

und es ist zunächst festzustellen, wieviele Wurzeln die Gleichung (3) mit (4) gemein hat.

Die sämtlichen Wurzeln von (3) sind aber nach § 69:

(5) $$j(p\,\omega),\quad j\left(\frac{\omega+\lambda}{p}\right),$$

wenn λ ein Restsystem nach dem Modul p durchläuft. Die erste von diesen gehört nicht zu den Wurzeln von (4), denn $\omega' = p\,\omega$ genügt der Gleichung:

$$a\,\omega'^2 + p\,b\,\omega' + p^{\varepsilon+2}c = 0,$$

die primitiv und von der Diskriminante $-mp^2$ ist. Wenn wir aber $p\,\omega' = \omega + \lambda$ setzen, so erhalten wir für ω' die Gleichung:

(6) $$a p^2 \omega'^2 + p(b - 2a\lambda)\,\omega' + (a\lambda^2 - b\lambda + cp^\varepsilon) = 0,$$

und diese Gleichungen sind ebenfalls von der Diskriminante $-mp^2$. Es sind aber zwei darunter, die imprimitiv vom Teiler p sind, nämlich die den Werten

(7) $$\lambda \equiv 0,\quad a\lambda - b \equiv 0 \pmod{p}$$

entsprechen. Die erste ist die Wurzel der Form $(ap, b, cp^{\varepsilon-1})$, die zweite die der Form

$$(ap,\ b - 2a\lambda,\ C),$$

und da $b - 2a\lambda \equiv b \pmod{2a}$ und [nach (7)] $\equiv -b \pmod{2p}$ ist, so ist diese Form komponiert aus (a, b, cp^ε) und $(p, -b, acp^{\varepsilon-1})$, die in die zu l reziproke Klasse l^{-1} gehört. Daraus ergibt sich:

I. Die Gleichungen (3) und (4) haben nur zwei Wurzeln miteinander gemein, nämlich die Klasseninvarianten (lk) und $(l^{-1}k)$, und wenn die Klasse l zweiseitig ist, so haben sie nur eine Wurzel gemein.

Setzt man also in (3) $u = (k)$, so ist der größte gemeinschaftliche Teiler von (3) und (4) vom zweiten, und wenn l zweiseitig ist, vom ersten Grade. Im ersteren Falle sind (lk) und $(l^{-1}k)$ die Wurzeln einer quadratischen Gleichung, deren Koeffizienten rational von u abhängen, und deren Form im übrigen nur von der Klasse l, nicht von k abhängig ist. Dem hiermit bewiesenen können wir den Ausdruck geben:

II. Es ist

(8) $$(lk) + (l^{-1}k) = f_l(k),$$

oder, wenn l zweiseitig ist,

(9) $$(lk) = f_l(k),$$

worin $f_l(k)$ eine rationale Funktion von (k) bedeutet, deren rationale Zahlenkoeffizienten nur von der Klasse l, nicht von der Klasse k abhängen.

Wir betrachten nun die Reihe der Klasseninvarianten

(10) $$\ldots, (l^{-2}k), (l^{-1}k), (k), (lk), (l^2k), (l^3k), \ldots,$$

die beliebig nach vorwärts und nach rückwärts fortgesetzt werden kann. In dieser Reihe ist, wenn l zum Exponenten ε gehört, $(l^\nu k)$ mit $(l^{\nu+\varepsilon}k)$ identisch, während alle zwischenliegenden Glieder davon und untereinander verschieden sind. Ist l zweiseitig, so enthält die Reihe (10) nur zwei verschiedene Glieder, von denen jedes durch das andere rational ausdrückbar ist. Anderenfalls schließen wir nach (8), daß jedes Glied der Reihe (10) rational ausdrückbar ist durch die beiden vorhergehenden (oder auch durch die beiden folgenden) in der Form

(11) $$(l^{\nu+1}k) = -(l^{\nu-1}k) + f_1(l^\nu k).$$

Durch eine wiederholte Anwendung dieser Formel gelangt man zu dem Satze, daß jedes Glied der Reihe (10) rational ausgedrückt werden kann durch irgend zwei aufeinanderfolgende Glieder derselben Reihe.

Ist aber l zweiseitig, so sind alle Glieder der Reihe (10) rational durch eines ausdrückbar.

§ 121. Trennung der entgegengesetzten Klassen.

Es kommt nun darauf an, auch im Falle eines nicht zweiseitigen l die beiden Wurzeln der quadratischen Gleichung voneinander zu trennen, was durch Adjunktion von $\sqrt{D}$ möglich ist.

Ist die Klasse l nicht zweiseitig, so sind die beiden Klasseninvarianten (lk), $(l^{-1}k)$ voneinander verschieden und daher (§ 118, III.)

$$v = (lk) = j\left(\frac{\omega}{p}\right)$$

eine einfache Wurzel der Transformationsgleichung

$$F_p(u, v) = 0$$

(§ 119, V.). Setzen wir also

(1) $$M = \left(\frac{\eta\left(\frac{\omega}{p}\right)}{\eta(\omega)}\right)^{24},$$

so folgt nach § 72, daß M rational durch

$$j(\omega) \quad \text{und} \quad j\left(\frac{\omega}{p}\right),$$

also rational durch (k) und (lk) ausdrückbar ist, und aus § 72 ergibt sich, daß M eine ganze algebraische Zahl ist.

Diesen Satz wenden wir an auf je zwei aufeinanderfolgende Glieder der Reihe (7) und erhalten, wenn wir

$$\omega_1 = \frac{\omega}{p}, \quad \omega_2 = \frac{\omega_1}{p}, \quad \ldots, \quad \omega_\varepsilon = \frac{\omega_{\varepsilon-1}}{p}$$

setzen, und wenn φ eine durch die Klasse l vollständig bestimmte rationale Funktion bedeutet:

$$(2) \qquad \begin{aligned} M &= \left(\frac{\eta(\omega_1)}{\eta(\omega)}\right)^{24} = \varphi(k, lk), \\ M_1 &= \left(\frac{\eta(\omega_2)}{\eta(\omega_1)}\right)^{24} = \varphi(lk, l^2 k), \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ M_{\varepsilon-1} &= \left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega_{\varepsilon-1})}\right)^{24} = \varphi(l^{\varepsilon-1} k, k). \end{aligned}$$

Durch Multiplikation aller dieser Gleichungen folgt:

$$(3) \qquad \left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega)}\right)^{24} = \varphi(k, lk)\,\varphi(lk, l^2 k) \ldots \varphi(l^{\varepsilon-1} k, k).$$

Nach § 120 kann aber die rechte Seite dieser Gleichung als rationale Funktion $\Phi(k, lk)$ von (k) und (lk) (mit rationalen Zahlkoeffizienten) dargestellt werden.

Andererseits ist, da l zum Exponenten ε gehört, l^ε mit der Hauptform, also $l^\varepsilon k$ mit k und ω_ε mit ω äquivalent, also besteht eine Gleichung:

$$(4) \qquad \omega_\varepsilon = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \alpha\delta - \beta\gamma = 1,$$

und es ist $\eta(\omega_\varepsilon) : \eta(\omega)$ nach § 38 zu bestimmen. Genügt, wie wir angenommen haben, ω der Gleichung

$$(5) \qquad a\omega^2 + b\omega + cp^\varepsilon = 0,$$

so erhält man aus (4), da $\omega_\varepsilon = \omega/p^\varepsilon$ ist:

$$\beta\omega^2 + (\alpha - p^\varepsilon\delta)\omega + \gamma p^\varepsilon = 0,$$

was durch Vergleichung mit (5) gibt

$$\beta = ax, \quad \alpha - p^\varepsilon\delta = bx, \quad \gamma = -cx,$$

und wenn man $\alpha + p^\varepsilon\delta = y$ setzt:

$$(6) \qquad \begin{aligned} \alpha &= \frac{y + bx}{2}, \quad \beta = ax, \\ p^\varepsilon\gamma &= -cx, \quad p^\varepsilon\delta = \frac{y - bx}{2}, \end{aligned}$$

also

$$4p^\varepsilon = y^2 + mx^2.$$

Daraus sind x und y bis auf die Vorzeichen bestimmt, und x kann positiv angenommen werden, und das Vorzeichen von y ergibt sich aus der Kongruenz

(7) $$y \equiv bx \pmod{p^\varepsilon}.$$

Betrachtet man dagegen die Komposition $l^{-1}k$, so hat man die Form (a, b, cp^ε) mit $(p, -b, acp^{\varepsilon-1})$ zu komponieren; man bestimmt b' aus den beiden Kongruenzen:

$$b' \equiv b \pmod{2a}, \qquad b' \equiv -b \pmod{2p^\varepsilon},$$

und es ist alles ebenso durchzuführen, nur daß an Stelle von (7) der Kongruenz

(8) $$y \equiv -bx \pmod{p^\varepsilon}$$

tritt, d. h. y bekommt das entgegengesetzte Zeichen.

Nach (5) und (6) ist aber

(9) $$\alpha + \beta\omega = \frac{y + (2a\omega + b)x}{2} = \frac{y + \sqrt{-m}\,x}{2},$$

worin, wenn a und x und folglich β positiv angenommen sind, $\sqrt{-m}$ positiv imaginär zu nehmen ist.

Es ist aber nach § 38, (4)

$$\left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega)}\right)^{24} = \left(\frac{y + \sqrt{-m}\,x}{2}\right)^{12},$$

und folglich erhält man nach (3)

(10) $$\Phi(k, lk) = \left(\frac{y + \sqrt{-m}\,x}{2}\right)^{12}.$$

Auf die gleiche Weise ergibt sich wegen (16):

(11) $$\Phi(k, l^{-1}k) = \left(\frac{y - \sqrt{-m}\,x}{2}\right)^{12},$$

und die Gleichung (10) ist daher nicht erfüllt, wenn (lk) durch $(l^{-1}k)$ ersetzt wird, außer wenn

(12) $$\left(\frac{y + \sqrt{-m}\,x}{2}\right)^{12} = \left(\frac{y - \sqrt{-m}\,x}{2}\right)^{12}$$

ist.

Dies ist aber nicht möglich, wenn, wie wir angenommen haben, p nicht in m aufgeht. Denn zerlegt man p im Körper $\Omega = \Re(\sqrt{D})$ in die zwei voneinander verschiedenen konjugierten Primideale $\mathfrak{p}, \mathfrak{p}'$, so geht das eine in $\frac{1}{2}(y + \sqrt{-m}\,x)$, das andere

in $\frac{1}{2}(y - \sqrt{-m}\,x)$ auf, und diese beiden Größen müssen also relativ prim sein. Folglich kann die Gleichung (12) nicht bestehen.

Die quadratische Gleichung, deren beide Wurzeln (lk), $(l^{-1}k)$ sind, hat also mit (18) nur eine Wurzel gemein, und daraus ergibt sich der wichtige Satz:

III. Nach Adjunktion von $\sqrt{D}$ ist (lk) rational ausdrückbar durch (k) in der Form:

(13) $$(lk) = f_l(k, \sqrt{D}),$$

wo f_l eine rationale Funktion ist, deren Form durch die Klasse l allein bestimmt ist.

Die Änderung des Zeichens von $\sqrt{D}$ hat den Erfolg, daß (lk) in $(l^{-1}k)$ übergeht, also:

$$f_l(k, \sqrt{D}) = f_{l^{-1}}(k, -\sqrt{D}).$$

Ist l zweiseitig, so gilt nach I. dieselbe Formel, nur daß $\sqrt{D}$ in f_l dann nicht vorkommt.

Ist l' eine zweite Klasse von derselben Beschaffenheit wie l, so kann man die Formel (13) auf $l'k$ anwenden und erhält:

$$(ll'k) = f_l(l'k, \sqrt{D}),$$

was mit Anwendung von

$$(l'k) = f_{l'}(k, \sqrt{D})$$

in eine Gleichung der Form:

$$(ll'k) = f_{ll'}(k, \sqrt{D})$$

übergeht. Da man auf der linken Seite l mit l' vertauschen kann, so folgt

$$f_{ll'}(k, \sqrt{D}) = f_{l'l}(k, \sqrt{D}),$$

so daß $f_{ll'}$ nur von der zusammengesetzten Klasse ll' abhängt. Ebenso läßt sich ableiten

$$(ll'l''k) = f_{ll'l''}(k, \sqrt{-m}),$$

und da nach § 118, II. jede beliebige Klasse s der Diskriminante D aus solchen Klassen l zusammensetzbar ist, so ist die Formel (13) nebst den daraus gezogenen Folgerungen nicht mehr an die über l gemachte besondere Voraussetzung gebunden, daß der erste Koeffizient eine Primzahl sei.

Wir haben also, wenn s, k zwei beliebige Klassen der Diskriminante D bedeuten, die Formeln:

(14) $$(sk) = f_s(k, \sqrt{D}),$$

(15) $$(s^{-1}k) = f_s(k, -\sqrt{D}).$$

Ist k die Hauptklasse, so ist

$$2\omega = \sqrt{D} \quad \text{oder} \quad 2\omega = -1 + \sqrt{D},$$

und da $\sqrt{D}$ rein imaginär ist, so ist $k = j(\omega)$ nach § 69 (4) reell. Demnach ergibt sich aus (14) und (15), da jetzt $(sk) = (s)$ wird:

Die Invarianten entgegengesetzter Klassen sind konjugiert imaginär, die Invarianten zweiseitiger Klassen sind reell.

Kehren wir zu einer beliebigen Klasse k zurück und setzen in der Formel (15) sk an Stelle von k, so folgt:

$$(16) \qquad (k) = f_s(sk, -\sqrt{D}),$$

oder, indem man $sk = k'$ setzt und f für f_s schreibt, nach (21)

$$(17) \qquad \begin{aligned} (k') &= f(k, \sqrt{D}), \\ (k) &= f(k', -\sqrt{D}), \end{aligned}$$

worin nun k, k' irgend zwei Klassen der Determinante D sein können.

Hiernach sind wir imstande, die Galoissche Gruppe der Klassengleichung, oder zunächst wenigstens eine Gruppe von Permutationen zu bestimmen, in der die Gruppe der Klassengleichung als Teiler enthalten ist.

Nehmen wir zunächst an, es sei die $\sqrt{D}$ dem Rationalitätsbereich der rationalen Zahlen adjungiert, und wenn $(k), (k'), (k'')\ldots$ die sämtlichen Klasseninvarianten der Diskriminante D bedeuten,

$$R(k, k', k'', \ldots)$$

irgend eine rationale Funktion dieser Größen. Nach unserem Satze läßt sich diese Funktion rational ausdrücken durch eine der Größen (k), also etwa:

$$R(k, k', k'', \ldots) = R'(k).$$

Bedeutet ferner (s) eine beliebige Klasseninvariante der Diskriminante D, und hat die Funktion R die Eigenschaft, durch die sämtlichen h Permutationen

$$\begin{pmatrix} k, & k', & k'', & \ldots \\ sk, & sk', & sk'', & \ldots \end{pmatrix},$$

deren Gesamtheit wir mit $\mathfrak{S}$ bezeichnen wollen, ungeändert zu bleiben, so ist $R'(k) = R'(sk)$, und daher rational ausdrückbar.

Die Galoissche Gruppe der Klassengleichung nach Adjunktion von $\sqrt{D}$ ist also in dem System $\mathfrak{S}$ enthalten,

und da $\mathfrak{S}$ eine Abelsche Gruppe ist, so ist die Klassengleichung eine Abelsche.

Nehmen wir an, die Funktion R habe reelle (rationale) Koeffizienten, so wird gleichwohl ihr rationaler Ausdruck die Form $a + b\sqrt{D}$ haben, worin a, b rationale Zahlen sind. Der imaginäre Teil wird dann und nur dann wegfallen, wenn R auch durch die Vertauschung sämtlicher Klassen $k, k', k'', \ldots$ mit ihren entgegengesetzten ungeändert bleibt. Daraus folgt, daß ohne Adjunktion von $\sqrt{D}$ die Galoissche Gruppe der Klassengleichung enthalten ist in dem System von $2h$ Permutationen, die man erhält, wenn man in $\mathfrak{S}$ jede Klasse in ihre entgegengesetzte verwandelt. Nur in dem besonderen Falle, in dem alle Klassen zweiseitig sind (der nur für eine endliche Anzahl von Determinanten stattfindet), ist dies letztere System mit $\mathfrak{S}$ identisch, und die Klassengleichung ist ohne Adjunktion von $\sqrt{D}$ eine Abelsche.

Der algebraische Körper, der aus den rationalen Funktionen einer Klasseninvariante gebildet ist, ist daher, von dem zuletzt erwähnten Ausnahmefall abgesehen, kein Normalkörper, sondern ist von seinen konjugierten Körpern verschieden. Dagegen erhält man einen Normalkörper, wenn man die Quadratwurzel $\sqrt{D}$ dem Körper der Klasseninvarianten adjungiert. Denn jede rationale Funktion sämtlicher Wurzeln der Gleichung kann durch eine von ihnen und $\sqrt{D}$ rational ausgedrückt werden.

§ 122. Irreducibilität.

Wir betrachten jetzt den algebraischen Zahlkörper

$$\mathfrak{K} = \mathfrak{R}(k, \sqrt{D}), \tag{1}$$

der aus einer Klasseninvariante (k) der Diskriminante D und $\sqrt{D}$ zusammengesetzt ist; in diesem Körper sind nach dem vorigen Paragraphen alle zu derselben Diskriminante gehörenden Klasseninvarianten $(k), (k'), (k''), \ldots$ enthalten. Diesen Körper nennen wir den Klassenkörper der Diskriminante D. Den quadratischen Körper $\mathfrak{R}(\sqrt{D})$ bezeichnen wir wie bisher mit Ω, der, wenn $D = Q^2 \Delta$ und Δ der Stamm von D ist, mit $\mathfrak{R}(\sqrt{\Delta})$ identisch ist. h sei die Klassenzahl der Diskriminante D.

1. Es sei (k) irgend eine der h Klassenvarianten und

$$\Phi(k) = (k)^{\nu} + \alpha_1 (k)^{\nu-1} + \alpha_2 (k)^{\nu-2} \cdots + \alpha_{\nu} = 0 \tag{2}$$

die Gleichung niedrigsten Grades in Ω, deren Wurzel (k) ist. Da (k) eine ganze Zahl ist, so müssen auch die α_i ganze Zahlen

des Körpers Ω sein (Bd. II, § 149). Es ist dann, wenn t eine Variable bedeutet, $\Phi(t)$ ein Divisor der Klassenfunktion $H_m(t)$, und folglich ist auch die Diskriminante von $\Phi(t)$ ein Teiler der Diskriminante von $H_m(t)$.

Ist ζ eine beliebige ganze Zahl des Körpers $\mathfrak{K}$, so ist die Relativspur in bezug auf Ω (Bd. II, § 175):

$$\mathfrak{S}\left(\frac{\zeta}{t-(k)}\,\Phi(t)\right) = \varphi(t)$$

eine ganze Funktion von t, höchstens vom Grade $\nu - 1$, deren Koeffizienten ganze Zahlen von Ω sind. Lassen wir also t in (k) übergehen, so folgt:

$$\zeta = \frac{\varphi(k)}{\Phi'(k)}, \tag{3}$$

und daraus:

$$b\zeta = \beta_0 + \beta_1(k) + \beta_2(k)^2 + \cdots + \beta_{\nu-1}(k)^{\nu-1}, \tag{4}$$

worin $\beta_0, \beta_1, \ldots, \beta_{\nu-1}$ ganze Zahlen in Ω sind, und b eine ganze rationale Zahl bedeutet, für die man die Diskriminante der Gleichung (2):

$$b = N[\Phi'(k)]$$

nehmen kann. Die Körperdiskriminante geht dann in b auf, und keine der in b nicht aufgehenden Primzahlen ist in Ω oder in $\mathfrak{K}$ durch das Quadrat eines Primideals teilbar (Bd. II, § 174). Die Zahl b hängt nicht von der besonderen Zahl ζ ab.

Eine ganze Zahl ζ ist nur auf eine Weise in der Form (4) darstellbar, weil sonst (k) einer Gleichung von niedrigerem als dem νten Grade genügen würde, was der Voraussetzung widerspricht; und daraus folgt, daß ζ nur dann durch eine ganze Zahl α des Körpers Ω teilbar ist, wenn alle Koeffizienten $\beta_0, \beta_1, \ldots, \beta_{\nu-1}$ durch α teilbar sind. Denn stellt man ζ/α in der Form (4) dar, so müssen die Koeffizienten in dieser Darstellung ebenfalls ganze Zahlen sein.

Ersetzen wir (k) in (3) durch eine andere Wurzel der Gleichung (2), so geht ζ in einen konjugierten Wert über, der ebenfalls eine ganze Zahl ist.

2. Nach dem Fermatschen Satze ist für jede beliebige Primzahl p, wenn a eine ganze rationale Zahl bedeutet:

$$a^p \equiv a \pmod{p}. \tag{5}$$

Ferner ist, wenn p nicht in $2D$ aufgeht, nach § 85

$$D^{\frac{p-1}{2}} \equiv (D, p) \pmod{p},$$

also:

$$\sqrt{D}^p \equiv (D, p)\sqrt{D} \pmod{p}. \tag{6}$$

Bezeichnet daher α wie oben eine ganze Zahl des Körpers Ω:

$$\alpha = \frac{x + y\sqrt{\Delta}}{2},$$

also, wenn man mit $2Q$ multipliziert, x für Qx schreibt und mit α' die zu α konjugierte Zahl bezeichnet:

$$2Q\alpha = x + y\sqrt{D}, \quad 2Q\alpha' = x - y\sqrt{D},$$

und daraus folgt nach dem Fermatschen Satze und nach (6):

$$\begin{matrix} \alpha^p \equiv \alpha, & (D, p) = +1, \\ \alpha^p \equiv \alpha', & (D, p) = -1, \end{matrix} \pmod{p}. \tag{7}$$

Daraus folgt nun, wenn $f(k, \sqrt{-m})$ irgend eine Zahl von der Form (4) ist, mit Anwendung des polynomischen Lehrsatzes:

$$\begin{matrix} f(k, \sqrt{D})^p \equiv f(k^p, \sqrt{D}), & (D, p) = +1, \\ f(k, \sqrt{D})^p \equiv f(k^p, -\sqrt{D}), & (D, p) = -1, \end{matrix} \pmod{p}, \tag{8}$$

worin k^p für $(k)^p$ steht, also die Bedeutung einer wirklichen Potenz hat.

3. Wenn $\mathfrak{P}$ ein in p aufgehendes Primideal in $\mathfrak{K}$ ist, so ist die Norm von $\mathfrak{P}$ eine Potenz von p:

$$N(\mathfrak{P}) = p^f. \tag{9}$$

Der Exponent f ist der Grad des Primideals $\mathfrak{P}$. Für jede beliebige ganze Zahl ζ des Körpers $\mathfrak{K}$ ist

$$\zeta^{N(\mathfrak{P})} \equiv \zeta \pmod{\mathfrak{P}}, \tag{10}$$

und wenn umgekehrt p^f die niedrigste Potenz von p ist, bei der die Kongruenz

$$\zeta^{p^f} \equiv \zeta \pmod{\mathfrak{P}} \tag{11}$$

durch jede Zahl ζ befriedigt wird, so ist f der Grad des Ideals $\mathfrak{P}$ (Bd. II, § 167).

Es sind nun die Grade der Primideale zu ermitteln, die in der Primzahl p enthalten sind.

Da p nicht in der Grundzahl des Körpers $\mathfrak{K}$ aufgeht, so ist p nicht durch das Quadrat eines Primideals teilbar.

4. Bedeuten $(k), (k'), \ldots, (k^{(h-1)})$ die sämtlichen Wurzeln der Gleichung

$$H_m(u) = 0,$$

so ist für ein variables t

$$H_m(t) = [t - (k)]\,[t - (k')] \ldots [t - (k^{(h-1)})],$$

und diese Funktion hat ganze rationale Koeffizienten. Es ist also nach (5):

$$[H_m(t)]^p \equiv H_m(t^p) \pmod{p},$$

also, wenn wir $t = (k)$ setzen:

$$[(k)^p - (k)]\,[(k)^p - (k')] \ldots [(k)^p - (k^{(h-1)})] \equiv 0 \pmod{p}.$$

Bedeutet also $\mathfrak{P}$ ein in p aufgehendes Primideal in $\mathfrak{K}$, so muß wenigstens einer der Faktoren der linken Seite durch $\mathfrak{P}$ teilbar sein, und daraus folgt eine Kongruenz

(12) $$(k)^p \equiv (k') \pmod{\mathfrak{P}},$$

worin (k') irgend eine der Klasseninvarianten ist, die auch mit (k) identisch sein kann.

5. Ist zunächst

$$(D, p) = -1,$$

so kann $\mathfrak{P}$ jedenfalls nicht vom ersten Grade sein, weil ja schon

(13) $$\left.\begin{aligned} \sqrt{D}^p &\equiv -\sqrt{D} \\ \sqrt{D}^{p^2} &\equiv \sqrt{D} \end{aligned}\right\} \pmod{\mathfrak{P}}$$

ist. Ist aber in (12) (nach § 121)

$$(k') = f(k, \sqrt{D}), \quad k = f(k', -\sqrt{D}),$$

so folgt aus (13)

$$(k')^p \equiv f(k^p, -\sqrt{D}) \equiv f(k', -\sqrt{D}) \equiv k,$$
$$(k)^{p^2} \equiv k \pmod{\mathfrak{P}},$$

und mithin ist für alle ganze Zahlen ζ des Körpers $\mathfrak{K}$

(14) $$\zeta^{p^2} \equiv \zeta \pmod{\mathfrak{P}},$$

und $\mathfrak{P}$ ist vom zweiten Grade.

6. Ist zweitens

$$(D, p) = +1,$$

so gibt es, wie in § 118 bewiesen ist, zwei entgegengesetzte Klassen l, l^{-1} (die, wenn l zweiseitig ist, miteinander identisch sind), die durch Formen mit dem ersten Koeffizienten p repräsentiert werden können, und wenn (k) eine beliebige Klasseninvariante ist, so ist nach § 120 die Invariantengleichung für den Transformationsgrad p:

(15) $$F_p(u, v) = 0$$

befriedigt für

$$u = (k),\ v = (l\,k) \quad \text{und} \quad v = (l^{-1}k).$$

Nach dem, was am Schlusse des § 69 bewiesen ist [Formel (32)], folgt aber hieraus die Kongruenz

(16) $$[(k)^p - (l\,k)]\,[(l\,k)^p - (k)] \equiv 0 \pmod{p}.$$

Wenn nun $\mathfrak{P}$ ein in p aufgehendes Primideal ist, so muß einer der beiden Faktoren auf der linken Seite von (17) durch $\mathfrak{P}$ teilbar sein. Welche der beiden hiernach möglichen Annahmen wir weiter verfolgen, ist gleichgültig, da die eine in die andere übergeht, wenn k mit $l^{-1}k$ und l mit l^{-1} vertauscht wird. Sei also

(17) $$(k)^p \equiv (l\,k) \pmod{\mathfrak{P}}.$$

Wenn die Kongruenz (17) für irgend einen der konjugierten Werte (k) befriedigt ist, so gilt sie auch für jeden anderen. Denn es ist nach § 121:

$$(k') = f(k, \sqrt{D}), \quad (l\,k') = f(l\,k, \sqrt{D}),$$

also

$$(k')^p \equiv f(k^p, \sqrt{D}) \equiv f(l\,k, \sqrt{D}) \equiv (l\,k') \pmod{\mathfrak{P}}.$$

Es folgt also aus (14), wenn man k durch $l^{-1}k$ ersetzt:

(18) $$(l^{-1}k)^p \equiv (k) \pmod{\mathfrak{P}},$$

d. h. je nachdem für l die eine oder die andere der beiden zu p gehörigen Klassen l gesetzt wird, ist der eine oder der andere Faktor von (16) durch $\mathfrak{P}$ teilbar.

Durch wiederholte Anwendung von (17) ergibt sich für jeden beliebigen positiven Exponenten π

(19) $$(k)^{p^\pi} \equiv (l^\pi k) \pmod{\mathfrak{P}}$$

(Schluß von π auf $\pi + 1$).

Wenn nun l zum Exponenten ε gehört, oder ε der Index von p ist, so ist nach (19):

(20) $$(k)^{p^\varepsilon} \equiv (k) \pmod{\mathfrak{P}},$$

und p^ε ist die niedrigste Potenz von p, die dieser Bedingung genügt. Denn wenn noch eine niedrigere Potenz von p die Kongruenz (19) erfüllt, so folgt aus (20), daß zwei verschiedene Klasseninvarianten (k), (k') nach dem Modul $\mathfrak{P}$ kongruent sind. Es wäre also ihre Differenz $(k) - (k')$ durch $\mathfrak{P}$ und mithin die Diskriminante von H_m durch p teilbar, gegen die Voraussetzung.

Daraus ergibt sich nun wieder nach (7), daß die Kongruenz

$$\xi^{p^e} \equiv \xi \pmod{\mathfrak{P}} \tag{21}$$

für jede ganze Zahl ξ in $\mathfrak{K}$ erfüllt ist und daraus also der Satz:

Eine Primzahl p zerfällt im Körper $\mathfrak{K}$ in lauter voneinander verschiedene Primideale, deren Grad gleich dem Index von p ist.

Wir wollen noch beweisen, daß es unter den verschiedenen in p aufgehenden Primidealen $\mathfrak{P}$ immer eines gibt, für welches von den beiden aus (16) folgenden Kongruenzen die Kongruenz (17) besteht.

Dazu bemerken wir: Wenn wir die sämtlichen Zahlen des Körpers $\mathfrak{K}$ in die konjugiert imaginären verwandeln, indem wir $\sqrt{D}$ mit $-\sqrt{D}$ und jede Klasseninvariante (k) mit der entgegengesetzten (k^{-1}) vertauschen, so gehen die sämtlichen Zahlen eines Ideals $\mathfrak{A}$ in die Zahlen eines konjugiert imaginären Ideals $\mathfrak{A}'$ über, das auch mit $\mathfrak{A}$ identisch sein kann, und die Norm des Ideals $\mathfrak{A}$ ist gleich der Norm des Ideals $\mathfrak{A}'$. Ist $\mathfrak{A}$ ein Primideal, so ist auch $\mathfrak{A}'$ ein Primideal.

Ist nun die Kongruenz (17) nicht erfüllt, so muß nach (16)

$$(l\,k)^p \equiv (k) \pmod{\mathfrak{P}}$$

sein, und auch diese Kongruenz bleibt bestehen, wenn k durch eine andere Klasse k' ersetzt wird. Setzen wir also $l^{-1}k^{-1}$ an Stelle von k, so folgt:

$$(k^{-1})^p \equiv (l^{-1}k^{-1}) \pmod{\mathfrak{P}}.$$

Da also $(k^{-1})^p - (l^{-1}k^{-1})$ eine Zahl in $\mathfrak{P}$ ist, so ist $(k)^p - (l\,k)$ in dem zu $\mathfrak{P}$ konjugierten Ideal $\mathfrak{P}'$ enthalten, und es ist

$$(k)^p \equiv (l\,k) \pmod{\mathfrak{P}'},$$

was aus (17) durch Vertauschung von $\mathfrak{P}$ mit $\mathfrak{P}'$ hervorgeht.

7. Aus diesen Sätzen ist die Irreducibilität der Klassengleichung auch nach Adjunktion von $\sqrt{D}$ eine einfache Folge.

Sind k, k' zwei beliebige Klassen der Diskriminante D, so können wir k' nach § 118 in der Weise zusammensetzen:

$$k' = k\,l\,l'\,l'' \ldots,$$

daß durch die Klassen $l, l', l'', \ldots$ die Primzahlen $p, p', p'', \ldots$ darstellbar sind. Nach dem, was soeben bewiesen ist, können wir also die Primteiler $\mathfrak{P}, \mathfrak{P}', \mathfrak{P}''$ dieser Primzahlen so wählen, daß

$$(22)\qquad \begin{aligned} (k)^p &\equiv (k\,l) & (\mathrm{mod}\ \mathfrak{P}),\\ (k\,l)^{p'} &\equiv (k\,l\,l') & (\mathrm{mod}\ \mathfrak{P}'),\\ (k\,l\,l')^{p''} &\equiv (k\,l\,l'\,l'') & (\mathrm{mod}\ \mathfrak{P}'')\\ &\ldots\ldots\ldots \end{aligned}$$

Nehmen wir jetzt an, es zerfalle die Klassengleichung, es sei also für ein variables t

$$H_m(t) = H_1(t)\, H_2(t),$$

so können wir, da k, k' beliebige Klassen waren, (k) unter den Wurzeln von $H_1(t)$, (k') unter denen von $H_2(t)$ wählen. In der Kette (22) gehört also das Anfangsglied (k) zu den Wurzeln (k_1) von $H_1(t)$ und das Endglied (k') zu den Wurzeln (k_2) von $H_2(t)$. Da mindestens an einer Stelle der Kette (22) der Übergang von den Wurzeln des einen Faktors zu denen des anderen stattfinden muß, so gibt es ein Paar von Wurzeln (k_1), (k_2), das für irgend eine Primzahl p und ein darin aufgehendes Primideal $\mathfrak{P}$ der Kongruenz

$$(k_1)^p \equiv (k_2) \quad (\mathrm{mod}\ \mathfrak{P})$$

genügt. Da nun $H_1(k_1) = 0$ ist, so folgt durch den oft angewandten Schluß

$$H_1(k_1)^p \equiv H_1(k_1^p) \equiv H_1(k_2) \equiv 0 \quad (\mathrm{mod}\ \mathfrak{P}).$$

Da nun

$$H_1(k_2) = \prod^{k_1} [(k_2) - (k_1)]$$

ist, so muß eine der Differenzen $(k_2) - (k_1)$ durch $\mathfrak{P}$ teilbar sein, was nicht möglich ist, da p nicht in der Diskriminante von H aufgeht.

Damit ist die Irreducibilität der Klassengleichung bewiesen; der Grad des Körpers $\mathfrak{K}$ ist gleich dem Doppelten der Klassenzahl h festgestellt, und die im vorigen Paragraphen gefundene Gruppe $\mathfrak{S}$ ist als die wahre Gruppe der Klassengleichung erkannt.

8. Hiernach können wir alle Primzahlen p, abgesehen von einer endlichen Anzahl von Ausnahmen (die in $2D$ oder der Diskriminante von H aufgehen) in ihre Primfaktoren im Körper $\mathfrak{K}$ zerlegen.

Ist $(D, p) = +1$, so zerfällt p und Körper Ω in zwei konjugierte Primideale ersten Grades. Ist p vom Index ε, so ist jedes in p aufgehende Primideal $\mathfrak{p}$ vom Grade ε. Ist also

$$p = \mathfrak{P}_1\, \mathfrak{P}_2 \ldots \mathfrak{P}_r,$$

so ist wegen 5. $N(\mathfrak{p}) = p^{2h}$, und folglich

$$2h = r\varepsilon.$$

Die Anzahl der Primfaktoren, in die p im Körper $\mathfrak{K}$ zerfällt, ist also gleich $2h/\varepsilon$.

Ist ferner $(D, p) = -1$, so sind die Primfaktoren von p vom zweiten Grade, und ihre Anzahl ist also $= h$.

9. Eine interessante Folgerung ziehen wir noch aus diesen Resultaten. Es sei $(D, p) = +1$ und ε der Index von p. Dann ist $4p^\varepsilon$ durch die Form $x^2 - Dy^2$ darstellbar und

$$p^\varepsilon = \mu\mu', \tag{23}$$

wenn zur Abkürzung

$$\mu = \frac{x + y\sqrt{D}}{2}, \quad \mu' = \frac{x - y\sqrt{D}}{2} \tag{24}$$

gesetzt wird. Wir wissen nun, daß p in lauter verschiedene Primideale vom Grade ε zerfällt. Da p ungerade ist, und x, y höchstens den gemeinschaftlichen Teiler 2 haben, so haben μ, μ' keinen gemeinsamen Primfaktor in $\mathfrak{K}$. Jedem Primideal $\mathfrak{P}$, das in μ aufgeht, entspricht ein davon verschiedenes (konjugiertes) Primideal $\mathfrak{P}'$, das aus $\mathfrak{P}$ dadurch entsteht, daß man für alle Zahlen von $\mathfrak{P}$ die konjugiert imaginären Zahlen setzt. Es ist also μ nicht nur durch $\mathfrak{P}$, sondern durch $\mathfrak{P}^\varepsilon$ teilbar.

Nach § 121 ist

$$\left(\frac{\eta(\omega_1)}{\eta(\omega)}\right)^2 \left(\frac{\eta(\omega_2)}{\eta(\omega_1)}\right)^2 \cdots \left(\frac{\eta(\omega_\varepsilon)}{\eta(\omega_{\varepsilon-1})}\right)^2 = \varrho\mu, \tag{25}$$

und nach § 72, 4 genügen die Faktoren P^2 auf der linken Seite dieses Ausdrucks einer Gleichung $P^2\varphi(P^2, \gamma_2, \gamma_3) = p$, worin $\varphi(P^2, \gamma_2, \gamma_3)$ eine ganze algebraische Zahl ist.

Daraus folgt aber, daß P^2 nicht durch eine höhere als die erste Potenz von $\mathfrak{P}$ teilbar sein kann, während doch μ durch $\mathfrak{P}^\varepsilon$ teilbar ist. Wir schließen also aus (25), daß jede der Zahlen P^2 durch die erste Potenz von $\mathfrak{P}$ teilbar sein muß, daß mithin alle diese Zahlen assoziiert sind. Bezeichnet also ϱ irgend eine algebraische Einheit, so ist

$$\frac{x + y\sqrt{-m}}{2} = \varrho P^{2\varepsilon},$$

also ist μ wirklich als εte Potenz einer im Körper $\mathfrak{K}$ existierenden Zahl dargestellt, und P^2 selbst ist eine Darstellung eines Primideals im Körper Ω durch ein Hauptideal im Körper $\mathfrak{K}$.

§ 123. Beziehungen zwischen Klasseninvarianten in den verschiedenen Ordnungen.

Zwischen den Klasseninvarianten verschiedener Diskriminanten $D = Q^2 \Delta$ mit dem gleichen Stamm Δ bestehen algebraische Beziehungen, die wir jetzt aufzusuchen haben.

Es sei p eine beliebige Primzahl (auch $p = 2$ nicht ausgeschlossen) und

(1) $$D' = p^2 D.$$

Es sei $-D = m$, $-D' = m'$, also $m' = p^2 m$, und

(2) $$H_m(u) = 0,$$

(3) $$H_{m'}(v) = 0$$

seien die zu den Diskriminanten $-m$, $-m'$ gehörigen Klassengleichungen.

$$v = j(\omega')$$

sei eine beliebige Wurzel der zweiten und

(4) $$A'\omega'^2 + B'\omega' + C' = 0, \quad B'^2 - 4A'C' = D'$$

die primitive quadratische Gleichung, der ω' genügt. A' möge, was erlaubt ist, durch p unteilbar vorausgesetzt sein.

Wir betrachten nun die Invariantengleichung

(5) $$F_p(u, v) = 0,$$

deren Wurzeln sind:

(6) $$u = j(p\omega'), \quad j\left(\frac{\omega' + c}{p}\right), \quad c = 0, 1, 2, \ldots, p-1.$$

Das Argument dieser Funktionen:

$$\omega = p\omega' \quad \text{oder} \quad = \frac{\omega' + c}{p}$$

genügt einer aus (4) abzuleitenden quadratischen Gleichung, nämlich:

(7) $$\omega = p\omega', \quad A'\omega^2 + B'p\omega + C'p^2 = 0,$$
$$\omega = \frac{\omega' + c}{p},$$
$$A'p^2\omega^2 + (B' - 2A'c)p\omega + A'c^2 - B'c + C' = 0.$$

Die Diskriminanten dieser Gleichungen sind $p^2 D' = p^4 D$, und die erste von ihnen ist immer primitiv, die Diskriminante

der zweiten Gleichung reduziert sich nur dann auf D, wenn sie imprimitiv ist und

$$\begin{aligned}(8)\qquad & B' - 2A'c \text{ durch } p,\\ & A'^2 c - B'c + C' \text{ durch } p^2\end{aligned}$$

teilbar ist, und dann genügt die entsprechende Zahl (6) gleichzeitig der Gleichung (5) und der Gleichung (2). Dies trifft aber, wie wir gleich zeigen, nur für einen Wert c zu, und folglich läßt sich der betreffende Wert u rational durch v ausdrücken.

Denn ist zunächst p ungerade, so hat die erste Kongruenz (8):

$$2A'c - B' \equiv 0 \pmod{p}$$

nur eine Wurzel, und für diese ist

$$(2A'c - B')^2 - p^2 D = 4A'(A'c^2 - B'c + C') \equiv 0 \pmod{p^2}.$$

Ist $p = 2$, so ist D' und folglich B' gerade und mithin $B' - 2A'c$ immer durch 2 teilbar. Es ist dann

$$\left(A'c - \frac{B'}{2}\right)^2 - D = A'(A'c^2 - B'c + C'),$$

und da $D \equiv 0$ oder $\equiv 1 \pmod{4}$ ist, so ist die linke Seite hier durch 4 teilbar, wenn $A'c - \frac{B'}{2} \equiv D \pmod{2}$ angenommen wird.

Geht man umgekehrt von einer Gleichung

$$(9)\qquad A\omega^2 + B\omega + C = 0,\quad B^2 - 4AC = D$$

der Diskriminante D aus, nimmt A relativ prim zu p an und setzt $\omega' = p\omega$, so genügt ω' der primitiven Gleichung

$$(10)\qquad A\omega'^2 + Bp\omega' + Cp^2 = 0$$

von der Diskriminante $D' = p^2 D$, und wenn wir also $v = j(\omega')$ setzen, so ist $u = j(\omega)$ rational durch v ausdrückbar. Daraus folgt also der Satz:

1. Jede Klasseninvariante für die Diskriminante D ist rational ausdrückbar durch eine Klasseninvariante für die Diskriminante $p^2 D$.

Um aber die Frage zu beantworten, wie viele Werte von v zu demselben Werte von $u = j(\omega)$ führen, bemerken wir, daß die verschiedenen Werte von v, die dies leisten, Wurzeln der Gleichung (5) und (3) sein müssen, also in einer der Formen

$$(11)\qquad j(p\omega),\quad j\left(\frac{\omega + c}{p}\right)$$

enthalten sind. Nun haben wir aus (9):

(12)
$$\omega' = p\,\omega, \quad A\,\omega'^2 + B\,p\,\omega' + C\,p^2 = 0,$$
$$\omega' = \frac{\omega + c}{p},$$
$$A\,p^2\,\omega'^2 + (B - 2\,A\,c)\,p\,\omega' + A\,c^2 - B\,c + C = 0,$$

deren Diskriminante D' ist. Unter den Größen (11) werden aber nur diejenigen der Gleichung (3) genügen, für die die entsprechende Gleichung (12) primitiv ist.

Die erste der Gleichungen (12) ist nach unserer Voraussetzung stets primitiv; von den übrigen sind nur die nicht primitiv, für die

(13)
$$A\,c^2 - B\,c + C \equiv 0 \pmod{p},$$

und von den Größen (11) fallen soviele aus, die nicht Lösungen von (3) sind, als die Kongruenz (13) Lösungen hat. Bezeichnen wir für den Augenblick die Zahl dieser Lösungen mit t, so ist die Anzahl der Werte von v, die zu demselben Wert von u gehören, $(p + 1 - t)$.

Nehmen wir zunächst $p = 2$, so haben wir, da A ungerade ist, folgende Fälle:

$$\begin{array}{llll} B \equiv 0, & & c \equiv C & \pmod{2}, \quad t = 1, \\ B \equiv 1, & C \equiv 0, & c \equiv 0, 1 & \pmod{2}, \quad t = 2, \\ B \equiv 1, & C \equiv 1 & & \pmod{2}, \quad t = 0, \end{array}$$

(weil $c^2 - c$ immer gerade ist). Dies läßt sich so zusammenfassen:

$$\begin{array}{ll} D \equiv 0 \pmod{4}, & t = 1, \\ D \equiv 1 \pmod{8}, & t = 2, \\ D \equiv 5 \pmod{8}, & t = 0. \end{array}$$

Mit Benutzung des Zeichens (D, p) (§ 85) können wir also setzen:

(14)
$$t = (D, p) + 1.$$

Ist p ungerade, so ist die Kongruenz (13) gleichbedeutend mit

$$(2\,A\,c - B)^2 \equiv D \pmod{p},$$

und diese hat eine Lösung $(2\,A\,c - B \equiv 0)$, wenn p in D aufgeht, wenn also $(D, p) = 0$ ist, zwei Lösungen, wenn D quadratischer Rest von p, also $(D, p) = +1$ ist, und keine Lösung, wenn D quadratischer Nichtrest, also $(D, p) = -1$ ist. Also gilt auch hier die Formel (14).

Nehmen wir daher vorläufig an, was wir gleich genauer untersuchen werden, es seien unter den $p + 1$ Größen

(15) $$p\,\omega, \quad \frac{\omega + c}{p}$$

keine zwei äquivalente, so gehören zu jedem Werte von u $[p - (D, p)]$ Werte v, und wenn wir die Grade von (2) und (3) mit h und h' bezeichnen, so ergibt sich (in Übereinstimmung mit den Formeln § 100) folgende Beziehung:

(16) $$h' = [p - (D, p)]\,h.$$

Nach § 122 sind h und h' die Klassenzahlen der Diskriminanten D, D'.

Es handelt sich also noch um die Frage, ob unter den Größen (15) nach Ausschluß der wegen (13) wegfallenden, noch äquivalente vorkommen können. Ist zunächst $p\,\omega$ äquivalent mit $\frac{\omega + c}{p}$, so ist:

(17) $$\frac{\omega + c}{p} = \frac{\gamma + \delta p \omega}{\alpha + \beta p \omega}, \quad \alpha\delta - \beta\gamma = 1,$$

oder:

(18) $$\beta p \omega^2 + (\alpha + \beta c p - \delta p^2)\,\omega + c\alpha - \gamma p = 0.$$

Diese Gleichung muß aus (9) durch Multiplikation mit einer ganzen Zahl g hervorgehen, und es folgt also:

$$\beta p = g A, \quad \alpha + \beta c p - \delta p^2 = g B, \quad c\alpha - g p = g C.$$

Da A durch p unteilbar angenommen war, so folgt hieraus, daß g und folglich α durch p teilbar ist. Setzen wir $g = p x$, $\alpha = p \alpha'$, so folgt:

(19) $$\beta = A x, \quad \alpha' + \beta c - \delta p = B x, \quad c\alpha' - \gamma = C x.$$

Setzen wir noch

(20) $$\alpha' - \beta c + \delta p = y,$$

so ergibt sich:

(21) $$\begin{aligned} 2\alpha' &= B x + y, \\ 2(\beta c - \delta p) &= B x - y, \end{aligned}$$

und aus

(22) $$p \alpha' \delta - \beta\gamma = 1$$

folgt sodann

(23) $$y^2 - D x^2 = 4.$$

Der Wert $x = 0$ ist auszuschließen, weil sonst $\beta = 0$ sein müßte, was der Gleichung (22) widerspricht, und wir können unbeschadet der Allgemeinheit x positiv annehmen. Da überdies D nach dem Modul 4 entweder $\equiv 0$ oder $\equiv 1$ ist, so

bleiben zur Erfüllung von (23) nur folgende zwei Möglichkeiten übrig:

1. $D = -3, \quad x = 1, \quad y = \pm 1.$

Da es für die Diskriminante -3 nur eine Formenklasse gibt, so können wir $A = 1$, $B = 1$, $C = 1$ annehmen, d. h. für ω die imaginäre dritte Einheitswurzel $e^{\frac{2\pi i}{3}}$ setzen, und erhalten unter den Größen (15) drei äquivalente, indem wir $y = +1$, und $= -1$ annehmen:

$$(24) \qquad p\,\omega, \quad \frac{\omega}{p}, \quad \frac{\omega + 1}{p},$$

wie auch aus den Gleichungen:

$$\frac{\omega}{p} = \frac{-1}{p + p\,\omega}, \quad \frac{\omega + 1}{p} = \frac{-1}{p\,\omega}$$

erkannt wird, aus denen die Äquivalenz der drei Größen (24) evident ist.

2. $D = -4, \quad x = 1, \quad y = 0.$

Wir können ebenso $B = 0$, $A = C = 1$, d. h. $\omega = i$ annehmen und finden die zwei äquivalenten Werte:

$$(25) \qquad p\,\omega, \quad \frac{\omega}{p},$$

wie auch aus der Gleichung:

$$p\,\omega = \frac{-p}{\omega}$$

folgt.

Es seien ferner zwei der Werte (3)

$$\frac{\omega + c}{p}, \quad \frac{\omega + c'}{p}$$

äquivalent, so daß eine Gleichung besteht:

$$(26) \qquad \frac{\omega + c}{p} = \frac{\gamma p + \delta(\omega + c')}{\alpha p + \beta(\omega + c')}, \quad \alpha\delta - \beta\gamma = 1,$$

oder

$$(27) \qquad \begin{gathered} \beta\,\omega^2 + (\beta\,c' + \beta\,c + \alpha p - \delta p)\,\omega + \\ \beta\,c\,c' + \alpha\,c\,p - \delta\,c' p - \gamma p^2 = 0, \end{gathered}$$

woraus durch Vergleichung mit (9)

$$(28) \qquad \begin{aligned} \beta &= A\,x, \\ \beta\,c' + \beta\,c + \alpha p - \delta p &= B\,x, \\ \beta\,c\,c' + \alpha\,c\,p - \delta\,c' p - \gamma p^2 &= C\,x, \end{aligned}$$

folgt, und wenn man wieder

(29) $$\beta c' - \beta c + \alpha p + \delta p = y$$

setzt:

(30) $$\begin{aligned} 2(\beta c' + \alpha p) &= Bx + y, \\ 2(\beta c - \delta p) &= Bx - y. \end{aligned}$$

Daraus

(31) $$y^2 - Dx^2 = 4p^2.$$

Aus (28) ergeben sich die Kongruenzen

(32) $$\begin{gathered} \beta c c' \equiv Cx, \quad \beta(c + c') \equiv Bx, \quad \beta \equiv Ax \\ Dx^2 \equiv \beta^2 (c - c')^2 \end{gathered} \pmod{p}.$$

Soll c' von c modulo p verschieden sein, so kann hiernach weder x noch D durch p teilbar sein und es folgt aus (32)

(33) $$\begin{aligned} A(c + c') &\equiv B, \\ A c c' &\equiv C, \end{aligned}$$

und dies führt durch Elimination von c' für c auf die Kongruenz (13), also auf den auszuschließenden Wert von c.

Fassen wir dies zusammen, so sehen wir, daß unter den Größen (15) nur in den beiden Ausnahmefällen $D = -3$, $D = -4$ äquivalente vorkommen, und zwar sind im Falle $D = -3$ je drei, im Falle $D = -4$ je zwei von ihnen äquivalent.

In diesen Fällen muß also die rechte Seite der Formel (16) noch durch 3 oder durch 2 geteilt werden, und die Formel bleibt also auch dann noch richtig, wenn man, wie schon früher, für $D = -3, -4$ unter h nicht 1, sondern $\frac{1}{3}$ und $\frac{1}{2}$ versteht.

§ 124. Klassenkörper und Ordnungskörper.

Ist $D = Q^2 \Delta$ eine Diskriminante und Δ ihr Stamm, so sind nach den Resultaten des vorigen Paragraphen die Klasseninvariante u der Diskriminante Δ rational durch die Klasseninvariante v der Diskriminante D ausdrückbar, und zu jedem u gehören r Werte von v, wenn r nach der Formel (16), § 123 bestimmt wird. Diese Werte von v sind die Wurzeln einer Gleichung $r$ten Grades, deren Koeffizienten rational von u abhängen. Die Größen v gehören also einem Körper $\mathfrak{K}(D)$ über $\mathfrak{K}(\Delta)$ an, der kein anderer ist als der Klassenkörper der Diskriminante D.

In bezug auf die quadratischen Körper $\Omega = \mathfrak{R}(\sqrt{\Delta})$ sind beide Körper Abelsche. Wir wollen, wenn eine genauere Unter-

scheidung nötig ist, den Körper $\mathfrak{K}(\Delta)$ den Klassenkörper von Ω, $\mathfrak{K}(D)$ den Klassenkörper für die Diskriminante D oder den Ordnungskörper für den Führer Q nennen.

Nach den Resultaten von § 122 ist, vielleicht mit einer endlichen Zahl von Ausnahmen,

> ein Primideal $\mathfrak{p}$ des Körpers Ω im Körper $\mathfrak{K}(\Delta)$ dann und nur dann in Primideale ersten Grades zerlegbar, wenn $\mathfrak{p}$ in Ω vom ersten Grade ist und der Hauptklasse angehört, also gleich einer komplexen Primzahl
>
> $$\pi = \frac{x + y\sqrt{\Delta}}{2}$$
>
> ist.
>
> Soll $\mathfrak{p}$ in $\mathfrak{K}(D)$ in Primideale ersten Grades $\mathfrak{P}$ zerlegt werden, so kommt noch hinzu, daß π der durch Q bestimmten Ordnung angehöre, d. h. nach dem Modul Q mit einer rationalen Zahl kongruent sei (§ 96).

Neunzehnter Abschnitt.

Berechnung der Klasseninvarianten.

§ 125. Die Klasseninvariante γ_2.

Wir haben schon oben bemerkt, daß außer der Funktion $j(\omega)$ noch andere Modulfunktionen zur Bildung von Klasseninvarianten geeignet sind, und oft zu einfacheren Resultaten Anlaß geben. Unter diesen tritt uns zunächst die Funktion $\gamma_2(\omega)$ entgegen, die durch $\sqrt[3]{j(\omega)}$ definiert ist.

Wir haben im § 71 gesehen, daß zwischen den Funktionen

(1) $$u = \gamma_2(\omega), \quad v = \gamma_2\left(\frac{c + \partial\omega}{a}\right),$$

falls $a\partial = n$ durch 3 nicht teilbar ist, und c durch 3 teilbar angenommen ist, eine Transformationsgleichung

(2) $$\Phi_n(u, v) = 0$$

besteht. Die Funktion Φ_n hängt aber nur von den beiden Argumenten $v u^{-n}$, u^3 ab, und in $\Phi_n(u, u) = 0$ kommt also, wenn $n \equiv 1 \pmod 3$ ist, nur u^3, d. h. $j(\omega)$ vor; in diesem Falle kann daher diese Gleichung kein anderes Resultat ergeben, als die Invariantengleichung. Anders ist es aber in dem Falle

(3) $$n \equiv -1 \pmod 3,$$

den wir jetzt voraussetzen wollen.

Wenn einer der Werte $v = u$ werden soll, so muß eine Relation bestehen

(4) $$\frac{\gamma + \delta\omega}{\alpha + \beta\omega} = \frac{c + \partial\omega}{a}, \quad \alpha\delta - \beta\gamma = 1,$$

und zugleich muß [§ 54, (15)]

(5) $$-\alpha\beta + \alpha\gamma + \beta\delta - \alpha^2\beta\delta \equiv 0 \pmod 3$$

sein. Es ist also jedenfalls ω Wurzel einer quadratischen Gleichung:

(6) $$A\omega^2 + B\omega + C = 0, \quad D = B^2 - 4AC.$$

Besteht umgekehrt eine solche Gleichung, so folgt durch Vergleichung mit (4) in der früher angewandten Art, wenn x, y ganze Zahlen sind:

$$
(7)\qquad
\begin{aligned}
\partial\beta &= Ax,\\
c\alpha - a\gamma &= Cx,\\
c\beta + \partial\alpha - a\delta &= Bx,\\
c\beta - \partial\alpha - a\delta &= y,
\end{aligned}
$$

woraus:

$$
(8)\qquad
\begin{aligned}
2\partial\alpha &= Bx - y,\\
2(c\beta - a\delta) &= Bx + y,\\
4n &= y^2 - Dx^2.
\end{aligned}
$$

Setzen wir A relativ prim zu $3n$ voraus, so muß $\partial = 1$, $a = n$ angenommen werden; denn nach (7) muß unter dieser Voraussetzung x durch ∂ teilbar sein, und folglich auch $c\alpha - a\gamma$ und $c\beta - a\delta$, woraus folgt, daß auch a, c durch ∂ teilbar sein müßten, während doch a, c, ∂ keinen gemeinsamen Teiler haben. Also ist

$$
(9)\qquad
\begin{aligned}
2\alpha &= Bx - y, & \beta &= Ax,\\
2n\gamma &= c(Bx - y) - 2Cx, & 2n\delta &= 2cAx - Bx - y.
\end{aligned}
$$

Die Zahlen x, y sind hier außer den in § 114, 1), 2) angegebenen Beschränkungen wegen (3) noch der unterworfen, daß $y^2 - Dx^2 \equiv -1 \pmod 3$ werde. Dadurch ist ausgeschlossen, daß D durch 3 teilbar sei. x muß von Null verschieden sein, und wir können es, ohne die Allgemeinheit zu beschränken, positiv annehmen. (Eine gleichzeitige Vorzeichenänderung von x und y bewirkt nur eine Vorzeichenänderung von α, β, γ, δ, die ohne Belang ist.)

Ist $D \equiv -1 \pmod 3$, so müssen x und y durch 3 unteilbar sein; ist $D \equiv 1 \pmod 3$, so ist y durch 3 teilbar, x nicht teilbar. Im übrigen können die Zahlen x, y beliebig angenommen werden. Es ist dann c bestimmt aus den beiden (miteinander verträglichen) Kongruenzen:

$$
\left.
\begin{aligned}
cAx &\equiv \frac{Bx + y}{2}\\
c\frac{Bx - y}{2} &\equiv Cx
\end{aligned}
\right\} \pmod n
$$

und kann, da n durch 3 unteilbar ist, noch der Bedingung

$$c \equiv 0 \pmod 3$$

unterworfen werden.

Nun ist nach (7) β durch 3 nicht teilbar, und daher reduziert sich die Kongruenz (5) durch Multiplikation mit β auf:

$$\alpha + \delta \equiv 0 \pmod 3$$

oder nach (7) und (3) auf

(10) $$B \equiv 0 \pmod 3.$$

Ersetzen wir in (6) ω durch $\omega \pm 1$, so geht B über in $B \pm 2A$, und von den drei Zahlen B, $B + 2A$, $B - 2A$ ist eine und nur eine durch 3 teilbar. Wir nehmen also an, es sei B selbst durch 3 teilbar, dann folgt, daß von den drei Werten

(11) $$\gamma_2(\omega),\quad \gamma_2(\omega+1) = e^{-\frac{2\pi i}{3}}\gamma_2(\omega),\quad \gamma_2(\omega-1) = e^{\frac{2\pi i}{3}}\gamma_2(\omega)$$

nur der erste der Gleichung

(12) $$\Phi_n(u, u) = 0$$

genügt. Die Gleichung (12) und

(13) $$u^3 - j(\omega) = 0$$

haben daher nur eine gemeinsame Wurzel, und diese ist rational durch $j(\omega)$ ausdrückbar. Damit ist bewiesen:

1. $\gamma_2(\omega)$ ist eine Klasseninvariante, wenn ω die Wurzel einer quadratischen Form ist, deren Diskriminante und erster Koeffizient durch 3 nicht teilbar sind, während der mittlere Koeffizient durch 3 teilbar ist.

Wenden wir dies Ergebnis auf den Fall $n = 2$ an, so erhalten wir zunächst aus der Gleichung (5), § 71:

(14) $$\Phi_2(u, u) = u^4 - 2u^3 - 495u^2 + 2^4 . 3^3 . 5^3 = 0.$$

Die Gleichung

$$y^2 - Dx^2 = 8$$

ist, da $D \equiv 0$ oder $\equiv 1 \pmod 4$ sein muß, nur für drei negative Werte von D lösbar, nämlich

(15) $$\begin{aligned} D &= -8, & x &= 1, & y &= 0,\\ D &= -7, & x &= 1, & y &= \pm 1,\\ D &= -4, & x &= 1, & y &= \pm 2. \end{aligned}$$

Diesen drei Werten von D entsprechend kann man für die Gleichung (6) die folgenden wählen:

$$\begin{aligned} D &= -8, & \omega^2 + 2 &= 0,\\ D &= -7, & \omega^2 + 3\omega + 4 &= 0,\\ D &= -4, & \omega^2 + 1 &= 0 \end{aligned}$$

oder

$$D = -8, \quad \omega = \sqrt{-2},$$
$$D = -7, \quad \omega = \frac{-3 + \sqrt{-7}}{2},$$
$$D = -4, \quad \omega = i.$$

Der Wert $\gamma_2(i)$ ist aber (nach § 117) bekannt, nämlich $= 12$, und daher muß die linke Seite von (14) durch $u - 12$ teilbar sein. Da dieser Faktor bekannt ist, findet man leicht die übrigen:
$$u^4 - 2u^3 - 495u^2 + 2^4 . 3^3 . 5^3 = (u - 12)(u - 20)(u + 15)^2.$$

Da $\gamma_2(\omega)$ ebenso wie $j(\omega)$ für ein rein imaginäres ω einen positiven Wert hat, so muß der Faktor $u - 20$ dem Werte $D = -8$ entsprechen, und wir erhalten:

(16) $$\gamma_2(i) = 12,$$

(17) $$\gamma_2(\sqrt{-2}) = 20,$$

(18) $$\gamma_2\left(\frac{-3 + \sqrt{-7}}{2}\right) = -15.$$

Es existieren außer -7 noch fünf ungerade durch 3 nicht teilbare negative Diskriminanten:

(19) $$-11, \quad -19, \quad -43, \quad -67, \quad -163\,[1],$$

für die es nur eine Formenklasse gibt. Für diese ist also nach unserem Satze:
$$-\gamma_2\left(\frac{-3 + \sqrt{-m}}{2}\right)$$
eine ganze rationale Zahl Z.

Um diese rationalen Zahlen zu finden, wollen wir Grenzen aufsuchen, zwischen denen sie liegen müssen, die um weniger als eine Einheit voneinander verschieden sind.

Nach § 54, (5), (8) ist:
$$\gamma_2(\omega) = f(\omega)^{16} - \frac{16}{f(\omega)^8} = f_1(\omega)^{16} + \frac{16}{f_1(\omega)^8}$$
$$= f_2(\omega)^{16} + \frac{16}{f_2(\omega)^8},$$
ferner nach § 34, (19):
$$f_2\left(\frac{-3 + \omega}{2}\right) f(\omega) = e^{-\frac{\pi i}{8}} \sqrt{2},$$

---

[1]) Daß nicht mehr Diskriminanten dieser Art existieren, kann bis jetzt nur daraus geschlossen werden, daß, soweit man die Berechnung der Klassenzahlen fortgesetzt hat, weitere Zahlen dieser Art nicht gefunden sind [vgl. die Tafel der Klassenzahlen von Gauss (Werke, Bd. II, S. 450)].

also

$$-\gamma_2\left(\frac{-3+\omega}{2}\right) = f(\omega)^8 - \frac{256}{f(\omega)^{16}}.$$

Setzt man also:

(20) $$q = e^{-\pi\sqrt{m}},$$

so erhält man [§ 24, (11)]:

$$Z = -\gamma_2\left(\frac{-3+i\sqrt{m}}{2}\right)$$

$$= q^{-\frac{1}{3}} \prod_{1,\infty}^{\nu} (1+q^{2\nu-1})^8 - \frac{256\, q^{\frac{2}{3}}}{\prod\limits_{1,\infty}^{\nu} (1+q^{2\nu-1})^{16}}.$$

Wir machen nun Gebrauch von der für jedes echt gebrochene positive x gültigen Grenzbestimmung:

$$1 + x < e^x < \frac{1}{1-x}, \quad e^{-x} > 1 - x,$$

und erhalten:

$$1 < \Pi(1+q^{2\nu-1}) < e^{\frac{q}{1-q^2}},$$

woraus

$$q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}} < Z < q^{-\frac{1}{3}} e^{\frac{8q}{1-q^2}} - 256\, q^{\frac{2}{3}} e^{-\frac{16q}{1-q^2}},$$

und indem man die obere Grenze noch vergrößert, kann man dafür auch setzen:

$$Z < q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}} + \frac{8\, q^{\frac{2}{3}}}{1 - 8\, q - q^2} + \frac{2^{12}\, q^{\frac{5}{3}}}{1-q^2}.$$

Für $m = 11$ ist q ungefähr $= 2^{-15}$, woraus man ersieht, daß der Unterschied beider Grenzen:

$$\frac{8\, q^{\frac{2}{3}}}{1 - 8\, q - q^2} + \frac{2^{12}\, q^{\frac{5}{3}}}{1-q^2}$$

bereits für $m = 11$ und noch mehr also für die größeren Werte von m sehr klein ist. Z ist also die zunächst über

$$q^{-\frac{1}{3}} - 256\, q^{\frac{2}{3}}$$

gelegene ganze Zahl, und dieser Wert, für die größeren m schon $q^{-\frac{1}{3}}$, kommen einer ganzen Zahl außerordentlich nahe. Daraus berechnet man diese Zahlen[1]):

[1]) Man tut gut, sich bei diesen und vielen der später beschriebenen Rechnungen ein- für allemal den Briggischen Logarithmus

$$\log(\pi \log e) = 0{,}134\,934\,184\,0$$

zu merken, bei dem man übrigens meist mit 7 Dezimalen ausreicht.

$$-\gamma_2\left(\frac{-3+\sqrt{-11}}{2}\right) = 32,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-19}}{2}\right) = 96 = 32.3,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-43}}{2}\right) = 960 = 64.15,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-67}}{2}\right) = 5280 = 32.3.5.11,$$

$$-\gamma_2\left(\frac{-3+\sqrt{-163}}{2}\right) = 640320 = 64.3.5.23.29.$$

Bei diesen Zahlen ist die Zerlegbarkeit in verhältnismäßig kleine Primzahlen bemerkenswert.

Auch für die Diskriminante -27 existiert nur eine Klasse. Da aber diese Diskriminante durch 3 teilbar ist, so ist nicht $\gamma_3(\omega)$, sondern erst $j(\omega)$ eine rationale Zahl. Man findet durch ähnliche Rechnung:

$$-j\left(\frac{-1+\sqrt{-27}}{3}\right) = 3.2^{15}.5^3.$$

§ 126. Die Klasseninvarianten $f(\omega)^{24}$.

Die Wurzeln der kubischen Gleichung

(1) $$(u-16)^3 - u j(\omega) = 0$$

sind, wie wir früher allgemein gesehen haben (§ 54),

$$u = f(\omega)^{24}, \quad -f_1(\omega)^{24}, \quad -f_2(\omega)^{24},$$

oder

(2) $$f(\omega)^{24}, \quad f(\omega+1)^{24}, \quad f\left(1-\frac{1}{\omega}\right)^{24}.$$

Es sei nun wieder ω die Wurzel der quadratischen Gleichung:

(3) $$A\omega^2 + B\omega + C = 0$$

mit der negativen Diskriminante:

(4) $$D = B^2 - 4AC,$$

worin A, B, C keinen gemeinschaftlichen Teiler haben, und $j(\omega)$ sei die Klasseninvariante. Setzen wir

$$\omega' = \omega + 1, \quad \omega'' = 1 - \frac{1}{\omega},$$

so ist

(5) $$\begin{gathered} A\omega'^2 + (B-2A)\omega' + (A-B+C) = 0, \\ A+B+C-(B+2C)\omega'' + C\omega''^2 = 0. \end{gathered}$$

Die drei Argumente von (2) sind also die Wurzeln von äquivalenten quadratischen Formen.

Wir unterscheiden die drei Fälle:

1. $D \equiv 0 \pmod 4$. Hier ist B gerade, und A und C können nicht beide gerade sein; von den drei Formen (3), (5) hat also die eine zwei ungerade äußere Koeffizienten, die beiden anderen haben einen geraden und einen ungeraden äußeren Koeffizienten.

2. Ist $D \equiv 1 \pmod 8$, so ist B ungerade $B^2 \equiv 1 \pmod 8$, $AC \equiv 0 \pmod 2$, also ist wenigstens einer der beiden Koeffizienten gerade, und unter den drei Formen (3), (5) ist eine, aber auch nur eine, die zwei gerade äußere Koeffizienten hat.

3. Ist $D \equiv 5 \pmod 8$, so ist $4AC \equiv 4 \pmod 8$ und die beiden äußeren Koeffizienten A und C sind ungerade.

Wenn es nun gelingt, eine ganzzahlige Gleichung aufzustellen, der von den drei Wurzeln (2) nur die eine genügt, so folgt daraus, daß diese eine Wurzel rational durch $j(\omega)$ ausdrückbar und also eine Klasseninvariante ist.

Es besteht zwischen den Funktionen

$$(6) \qquad u = f(\omega)^{24}, \quad v = f\left(\frac{c + \partial\omega}{a}\right)^{24} \quad (c \equiv 0) \pmod 2$$

für einen ungeraden Transformationsgrad n (§§ 73, 74) eine Transformationsgleichung:

$$\Phi_n(u, v) = 0,$$

und die Gleichung:

$$(7) \qquad \Phi_n(u, u) = 0$$

ist also nach § 53 nur dann befriedigt, wenn für eine der Größen (6):

$$(8) \qquad \frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

worin

$$(9) \text{ oder } \qquad \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix} \pmod 2$$
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} \equiv \begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix} \pmod 2$$

eine zur ersten oder zur zweiten Klasse (§ 36) gehörige lineare Transformation ist.

Die Vergleichung von (8) mit (3) führt aber, wie oben, zu den Bedingungen:

$$\begin{aligned}
&\beta \partial = A x, \\
&\alpha c - \gamma a = C x, \\
&\beta c - \delta a + \alpha \partial = B x, \\
(10) \qquad &\beta c - \delta a - \alpha \partial = y, \\
&\beta c - \delta a = \frac{Bx + y}{2}, \quad \alpha \partial = \frac{Bx - y}{2}, \\
&4n = y^2 - D x^2.
\end{aligned}$$

Nehmen wir A und n ohne gemeinsamen Teiler an, so muß $\partial = 1$, $a = n$ sein, denn eine in x und ∂ aufgehende Primzahl müßte auch in y und folglich in $\alpha c - \gamma a$ und $\beta c - \delta a$ und, wegen $\alpha\delta - \beta\gamma = 1$, auch in a und c aufgehen, während doch a, c, ∂ keinen gemeinsamen Teiler haben sollen. Aus (10) wird α, β, γ, δ, c ebenso bestimmt, wie im vorigen Paragraphen. Es ergeben sich zunächst die beiden Kongruenzen

$$c A x \equiv \frac{Bx + y}{2}, \quad c \frac{Bx - y}{2} \equiv C x \pmod{n},$$

von denen die eine aus der anderen folgt, wenn x teilerfremd zu n ist, und die Bedingung

$$c \equiv 0 \pmod{2}$$

ist damit verträglich. Weiter folgt:

$$(11) \qquad \begin{aligned}
\alpha &= \frac{Bx - y}{2}, & n\gamma &= -Cx + c\frac{Bx - y}{2}, \\
\beta &= A x, & n\delta &= -\frac{Bx + y}{2} + Acx.
\end{aligned}$$

Wenn nun D und mithin B ungerade ist, so müssen, da wegen (9) α und δ beide gerade oder beide ungerade sind, x und y gerade sein; also sind β und γ gerade, und α und δ müssen ungerade sein. Folglich muß von den beiden Zahlen $\frac{1}{2}x$, $\frac{1}{2}y$ eine gerade, eine ungerade sein. Das ist aber unabhängig davon, wie sich A und C gegen den Modul 2 verhalten.

Wenn also von den drei Größen (2) die eine der Gleichung (7) genügt, so tun es auch die beiden anderen, und wir können diese drei nicht voneinander trennen.

Wir müssen daher B gerade annehmen und setzen zur Vereinfachung:

$$(12) \qquad D = -4m,$$

worin m eine positive ganze Zahl ist.

Wir unterscheiden:

1. Wenn $D \equiv 4 \pmod 8$ ist, setzen wir

$$n = m, \quad x = 1, \quad y = 0,$$
$$\alpha = \frac{B}{2}, \quad \beta = A,$$
$$\gamma \equiv -C, \quad \delta \equiv \frac{B}{2} \pmod 2.$$

Die Kongruenz (9) fordert also, da nicht alle drei Koeffizienten A, B, C gerade sein können, daß die beiden äußeren Koeffizienten ungerade, der mittlere durch 4 teilbar sei, und dies findet nur für eine der drei Formen (3), (5) statt; folglich genügt eine der drei Funktionen (2) der Gleichung (7), und ist also Klasseninvariante.

2.
$$D \equiv 0 \pmod 8,$$
$$n = m + 1, \quad x = 1, \quad y = \pm 2,$$
$$\alpha = \frac{B}{2} - 1, \quad \beta = A,$$
$$\gamma \equiv -C, \quad \delta \equiv \frac{B}{2} + 1 \pmod 2.$$

Es müssen also auch hier die beiden äußeren Koeffizienten ungerade $B \equiv 2 \pmod 4$ sein, und es verhält sich dann alles wie oben. Damit ist bewiesen:

1. Ist ω die Wurzel einer primitiven quadratischen Gleichung mit negativer, durch 4 teilbarer Diskriminante D und ungeraden äußeren Koeffizienten, so ist $f(\omega)^{24}$ Klasseninvariante für die Diskriminante D.

Die Annahme, daß A relativ prim zu n, d. h. zu $m + 1$ oder zu m sei, kann nachträglich als unwesentlich aufgegeben werden.

Denn wenden wir auf ω eine lineare Transformation (S) an, so geht die Gleichung (3) bei ungeraden A, C in eine äquivalente Gleichung über, in der die äußeren Koeffizienten dann und nur dann beide ungerade sind, wenn (S) zur ersten oder zweiten Klasse gehört, also wenn $f(\omega)^{24}$ durch (S) ungeändert bleibt. Man kann dann noch (S) so bestimmen, daß der erste Koeffizient in der umgeformten Gleichung (3) zu einer beliebigen Zahl, also auch zu n relativ prim wird.

Auf den Fall $m = 1$ ist dies Verfahren nicht anwendbar, weil $\Phi_n(u, u)$ für $n = 1$, $\omega = i$ (aber auch nur für diesen Wert) identisch verschwindet, für $m = 1$ haben wir aber bereits früher gefunden (§ 83):

$$f(i)^{24} = 64,$$

so daß also auch in diesem Falle der ausgesprochene Satz gilt.

Wenn m ungerade ist, so ist bei ungeradem A, C der mittlere Koeffizient B durch 4 teilbar; dagegen ist bei geradem m unter der gleichen Voraussetzung B nicht durch 4 teilbar. Durch die Substitution $\omega + 1$ für ω erreichen wir aber auch im Fall eines geraden m, daß B durch 4 teilbar wird; dann aber wird auch C gerade. Durch die Vertauschung $(\omega, \omega + 1)$ geht aber $f(\omega)^{24}$ in $-f_1(\omega)^{24}$ über, so daß wir also unserem Satz auch den folgenden Ausdruck geben können:

2. Ist ω die Wurzel der quadratischen Gleichung:

$$A\omega^2 + B\omega + C = 0,$$

worin A ungerade, B gerade ist, so ist, je nachdem $D \equiv 4$ oder $D \equiv 0 \pmod 8$ ist, $f(\omega)^{24}$ oder $f_1(\omega)^{24}$ Klasseninvariante.

Da A und C nicht beide gerade sein können, so sind nur drei Fälle möglich, von denen durch die Vertauschungen

$$(\omega, \omega + 1), \quad \left(\omega, -\frac{1}{\omega}\right)$$

der zweite auf den ersten und der dritte auf den zweiten zurückgeführt wird. Wir haben also in diesen Fällen:

$$(13) \quad \begin{array}{llll} A \equiv 1, & C \equiv 1 \pmod 2, & \text{Klasseninvariante} & f(\omega)^{24}, \\ A \equiv 1, & C \equiv 0 \quad \text{„} & \text{„} & f_1(\omega)^{24}, \\ A \equiv 0, & C \equiv 1 \quad \text{„} & \text{„} & f_2(\omega)^{24}. \end{array}$$

Insbesondere ist also, wenn wir die Hauptform der Diskriminante $-4m$, $(1, 0, m)$, zugrunde legen, $f(\sqrt{-m})^{24}$ bei ungeradem und $f_1(\sqrt{-m})^{24}$ bei geradem m eine Klasseninvariante. Diese beiden Zahlen haben einen reellen positiven Wert, und sollen in den weiter unten folgenden Rechnungen vorzugsweise berücksichtigt werden.

Aus der Gleichung (1) schließen wir (Bd. II, § 154, 11.), da $j(\omega)$ eine ganze algebraische Zahl ist, daß auch $f(\omega)^{24}$ eine ganze algebraische Zahl sein muß, und die Form der Gleichung (1) zeigt, daß die Norm dieser Zahl eine Potenz von 2 ist.

§ 127. Die Potenzen von $f(\omega)$ als Klasseninvarianten.

Nach der Definition von $\gamma_2(\omega)$ ist:

(1) $$f(\omega)^8 = \frac{f(\omega)^{24} - 16}{\gamma_2(\omega)}.$$

Ist ω die Wurzel einer Gleichung:

(2) $$A\omega^2 + 2B\omega + C = 0, \quad AC - B^2 = m,$$

deren Diskriminante $-4m$ durch 3 nicht teilbar ist, so können wir, wenn nötig, durch Übergang zu einer äquivalenten Gleichung, A, C als ungerade, A durch 3 unteilbar und B durch 3 teilbar voraussetzen. Dann aber sind nach den beiden vorigen Paragraphen $f(\omega)^{24}$ und $\gamma_2(\omega)$ Klasseninvarianten, und wir erhalten aus (1) den Satz:

3. Ist ω Wurzel einer quadratischen Form von negativer, durch 3 nicht teilbarer Diskriminante, deren beide äußere Koeffizienten ungerade, deren mittlerer Koeffizient durch 6 teilbar ist, so ist
$$f(\omega)^8$$
eine Klasseninvariante.

Um die Frage zu untersuchen, ob auch noch niedrigere Potenzen von $f(\omega)$ Klasseninvarianten sein können, machen wir Gebrauch von der Formel:

(3) $$f(\omega + 2r)^6 = i^{-r} f(\omega)^6,$$

worin r eine ganze Zahl ist; die Werte
$$\omega_r = \omega + 2r$$
sind die Wurzeln von äquivalenten quadratischen Gleichungen
$$A\omega_r^2 + 2B_r\omega_r + C_r = 0,$$
worin

(4) $$B_r = B - 2Ar,$$

und hierin läßt sich r nach dem Modul 4 so bestimmen, daß bei ungeradem m:

(5) $$B_r \equiv 0, 2, 4, 6 \pmod 8$$

und bei geradem m:

(6) $$B_r \equiv 1, 3, 5, 7 \pmod 8.$$

Wenn es nun gelingt, eine Gleichung mit rationalen Koeffizienten aufzufinden, der von den vier Werten (3) entweder nur

der eine, der dem Werte $r = 0$ oder zwei, die den Werten $r = 0, 2$ entsprechen, genügen, so folgt, daß $f(\omega)^6$ oder $f(\omega)^{12}$ Klasseninvarianten sind.

Ist außerdem m durch 3 unteilbar, so kann man die B_r alle durch 3 teilbar voraussetzen, und es folgt dann durch Kombination mit dem Satz 1., daß auch

$$f(\omega)^8 f(\omega)^{-6} = f(\omega)^2 \quad \text{oder} \quad f(\omega)^{12} f(\omega)^{-8} = f(\omega)^4$$

unter den Klasseninvarianten enthalten sind.

Nachdem so unser nächstes Ziel bezeichnet ist, machen wir von dem Ergebnis des § 73 Gebrauch, daß zwischen

$$v = f\left(\frac{c + \partial\omega}{a}\right)^3, \quad u = f(\omega)^3$$

eine Modulargleichung:

$$\Phi_n(u, v) = 0 \tag{7}$$

besteht, wenn

$$a\partial = n, \quad c \equiv 0 \pmod{16}$$

ist. Die hieraus abgeleitete Gleichung

$$\Phi_n(u, u) = 0 \tag{8}$$

ist dann und nur dann befriedigt, wenn

$$\frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \tag{9}$$

worin $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ eine lineare Transformation der ersten oder zweiten Klasse ist, die [nach § 40, (12)] der Bedingung genügt:

$$\left(\frac{2}{\alpha - \beta}\right) e^{-\frac{\pi i}{8}(\alpha - \beta)(\alpha + \beta + \gamma - \delta)} = 1,$$

oder der damit gleichbedeutenden:

$$\alpha\gamma + \beta\delta + 2\alpha^2 - 2\alpha\beta - 2\alpha\delta \equiv 0 \pmod{16}. \tag{10}$$

Aus (9) folgt aber, wenn ω der Gleichung (2) genügt, wie wir im vorigen Paragraphen gesehen haben,

$$\begin{aligned} & n = y^2 + m x^2, \\ & \alpha = Bx - y, \quad n\gamma = -Cx + c(Bx - y), \\ & \beta = Ax, \qquad n\delta = -Bx - y + Acx. \end{aligned} \tag{11}$$

Nehmen wir zunächst m ungerade an, so können wir $n = m$, also $x = 1$, $y = 0$ setzen, und da c durch 16 teilbar ist, folgt:

$$\alpha = B, \quad \beta = A, \quad \gamma \equiv -mC, \quad \delta \equiv -mB \pmod{8},$$

also ergibt (10):

$$(12)\qquad B\left(m\frac{A+C}{2}-(m+1)B+A\right)\equiv 0 \pmod 8.$$

Wenn nun $m \equiv 3 \pmod 4$, so ist $A + C \equiv 0 \pmod 4$ und der in (12) in der Klammer stehende Ausdruck ungerade, daher ist (12) nur unter der Voraussetzung befriedigt, daß

$$B \equiv 0 \pmod 8.$$

Wir wollen, um Wiederholungen zu vermeiden, bei den im folgenden auszusprechenden Theoremen ein- für allemal voraussetzen, daß ω die Wurzel einer solchen Gleichung (3) der Diskriminante $-4m$ sei, in der A ungerade, B durch 8 teilbar sei. Damit ist also das Theorem bewiesen:

4. Ist $m \equiv 3 \pmod 4$, so ist $f(\omega)^6$ Klasseninvariante.

Ist ferner $m \equiv 5 \pmod 8$, so reduziert sich die Kongruenz (12) auf:

$$B\left(\frac{5C-A}{2}+2B\right)\equiv 0 \pmod 8,$$

und diese Bedingung ist erfüllt, wenn B durch 4 teilbar ist, dagegen nicht erfüllt, wenn B nur durch 2, nicht durch 4 teilbar ist. Daraus folgt:

5. Ist $m \equiv 5 \pmod 8$, so ist $f(\omega)^{12}$ Klasseninvariante.

Ist $m \equiv 1 \pmod 8$, so läßt sich aus der Kongruenz (12) nichts schließen. Dies stimmt mit dem Umstande überein, daß in diesem Falle $\Phi_m(u, u)$ nur von u^8 abhängig ist. Um auch hier zu ähnlichen Resultaten zu gelangen, wenden wir die Transformation zweiter Ordnung an. Wir nehmen in (7):

$$(13)\qquad n \equiv 1 \pmod 8$$

und setzen:

$$uv = \pm\sqrt{2}^3,$$

d. h.:

$$f\left(\frac{c+\partial\omega}{a}\right)^3 f(\omega)^3 = \pm\sqrt{2}^3,$$

oder [§ 34, (18)]:

$$(14)\qquad f\left(\frac{c+\partial\omega}{a}\right)^3 = \pm f\left(\frac{\omega-1}{\omega+1}\right)^3.$$

Die Gleichung (7) geht dadurch über in eine Gleichung:

$$(15)\qquad \Phi_n\left(u, \frac{\pm\sqrt{2}^3}{u}\right)=0,$$

oder genauer gesagt, je nach der Wahl des Vorzeichens in zwei Gleichungen, die außer dem Produkt

$$\sqrt{2}\, f(\omega)^2$$

nur rationale Zahlkoeffizienten enthalten. Letzteres ersieht man daraus, daß in der Gleichung (7) nur solche Produkte $u^h v^k$ vorkommen, in denen $h + k$ gerade ist (vgl. den Anfang von § 74).

Die Relation (14) fordert nun, daß ω einer Gleichung

$$(16) \qquad \frac{c + \partial \omega}{a} = \frac{\gamma(\omega + 1) + \delta(\omega - 1)}{\alpha(\omega + 1) + \beta(\omega - 1)}$$

genüge, in der $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ eine zur ersten oder zweiten Klasse gehörige lineare Transformation ist. Damit aber eine der beiden Gleichungen (14) wirklich erfüllt sei, ist nach § 40, (12) noch erforderlich:

$$(17) \qquad (\alpha - \beta)(\alpha + \beta + \gamma - \delta) \equiv 0 \pmod 8.$$

Nun folgt aber, wenn ω Wurzel der quadratischen Gleichung (2) ist, aus (16) wie oben:

$$(18) \qquad \begin{aligned} \partial(\alpha + \beta) &= A x, \\ \partial(\alpha - \beta) &= B x + y, \\ c(\alpha - \beta) - a(\gamma - \delta) &= C x, \\ c(\alpha + \beta) - a(\gamma + \delta) &= B x - y, \\ 2n &= y^2 + m x^2. \end{aligned}$$

Ist nun, wie vorausgesetzt war,

$$m \equiv 1 \pmod 8,$$

so setzen wir:

$$n = \frac{m+1}{2} \quad \text{oder} \quad \frac{m+9}{2},$$

je nachdem $m \equiv 1$ oder $\equiv 9 \pmod{16}$ ist, so daß auch $n \equiv 1 \pmod 8$ wird, dann ist $x = 1$, $y = \pm 1$ oder $= \pm 3$ zu setzen, und wenn wir A relativ prim zu n voraussetzen, so wird $\partial = 1$, $a = n$, und aus (18) folgt:

$$\begin{aligned} \alpha + \beta &= A, & n(\gamma - \delta) &= -C + c(B + y), \\ \alpha - \beta &= B + y, & n(\gamma + \delta) &= -B + y + cA. \end{aligned}$$

Hiernach ergibt die Bedingung (17), da $B + y$ ungerade, $c \equiv 0 \pmod{16}$ ist:

$$A \equiv C \pmod 8,$$

was nur möglich ist, wenn $B \equiv 0 \pmod 4$ ist. Um aber zu entscheiden, welche der beiden Gleichungen (15) erfüllt ist, kommt es nach § 40, (12) darauf an, ob

$$(\alpha - \beta)^2 - 1 + (\alpha - \beta)(\alpha + \beta + \gamma - \delta)$$

oder, was dasselbe ist,

$$(B + y)^2 - 1 + (B + y)(A - n\,C)$$

durch 16 oder nur durch 8 teilbar ist. Vermehrt man aber in diesem Ausdruck B um ein ungerades Vielfache von 4, so verändert er sich um ein ungerades Vielfache von 8, woraus zu schließen, daß, je nachdem $B \equiv 0$ oder $\equiv 4 \pmod 8$, die eine oder die andere der beiden Gleichungen (15) befriedigt ist.

Damit ist bewiesen:

6. Ist $m \equiv 1 \pmod 8$, so ist $\sqrt{2}\,f(\omega)^6$ Klasseninvariante.

In den Fällen, wo $m \equiv 3 \pmod 4$ ist, können wir noch einen Schritt weiter gehen. Wir haben in § 73 neben den Schlaeflischen Modulargleichungen auch die Gleichungen

$$\Phi_n(u_1, v_1) = 0 \tag{19}$$

kennen gelernt, die zwischen

$$u_1 = f_1(\omega)^3, \quad v_1 = \left(\frac{2}{a}\right) f_1\left(\frac{c + \partial\,\omega}{a}\right)^3 \tag{20}$$

bestehen, und aus § 73, (10), (15) ergibt sich, daß, wenn $n \equiv 7 \pmod 8$ vorausgesetzt wird, $\Phi_n(u_1, v_1)$ rational durch

$$u_1 v_1, \quad u_1^8 + v_1^8$$

dargestellt werden kann. Wenn wir also in (19)

$$v_1 = f_1\left(\frac{c + \partial\,\omega}{a}\right)^3 = \pm f_2(\omega)^3, \quad u_1 = f_1(\omega)^3 \tag{21}$$

setzen, so wird

$$u_1 v_1 = \frac{\pm\sqrt{2}^3}{f(\omega)^3},$$

und $u_1^8 + v_1^8$ kann rational durch $f(\omega)^{24}$ ausgedrückt werden [§ 34, (11)], d. h. es geht

$$\Phi_n(u_1, v_1) = 0$$

in eine oder, nach der Wahl des Vorzeichens, zwei rationale Gleichungen für

$$\xi = \sqrt{2}\,f(\omega)^3$$

über, die wir mit

$$F(\pm\,\xi) = 0 \tag{22}$$

bezeichnen wollen.

Die Gleichung (22) hat aber wieder eine Gleichung der Form (21) zur Folge, so daß in beiden die Vorzeichen übereinstimmen, und die Gleichung (21) fordert nach § 40, (7):

$$(23) \qquad \frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}, \quad \delta \equiv 0 \pmod{2},$$
$$\gamma^2 - 1 + \gamma(2\alpha - \delta) \equiv 0 \text{ oder } \equiv 8 \pmod{16},$$

und zwar gilt, je nachdem die eine oder die andere Kongruenz stattfindet, in (21) und (22) das eine oder das andere Vorzeichen.

Nehmen wir $m = n$, also $m \equiv -1 \pmod 8$, so ergibt sich aus (2) und (23) ganz wie oben:

$$\beta = A, \quad n\gamma = -C + cB,$$
$$\alpha = B, \quad n\delta = -B + cA,$$

also aus der zweiten Kongruenz (23):

$$C^2 + CB - 1 \equiv 0 \text{ oder } \equiv 8 \pmod{16},$$

woraus zunächst folgt, daß B jedenfalls durch 8 teilbar sein muß; vermehren wir aber B um ein ungerades Vielfache von 8, so geht die eine dieser Kongruenzen in die andere über, und infolgedessen geht in (21) das eine in das andere Vorzeichen über. Für ein bestimmtes ω besteht also nur die eine der beiden Gleichungen (22) und es folgt:

7. Ist $m \equiv 7 \pmod 8$, so ist $\sqrt{2}\,f(\omega)^3$ Klasseninvariante.

Wenn wir einer durch alle bekannten Beispiele bestätigten Induktion vertrauen dürfen, so besteht noch das folgende Theorem:

8. Ist $m \equiv 3 \pmod 8$, so ist $f(\omega)^3$ Klasseninvariante.

Indessen fehlt hierfür noch der allgemeine Beweis.

Ist $m \equiv 2 \pmod 4$, so wenden wir dasselbe Verfahren an, wie oben im Falle $m \equiv 1 \pmod 8$.

Wir setzen:

$$(24) \qquad 2n = m + y^2,$$

und nehmen $y = 0$ oder $= \pm 2$, so daß $n \equiv 1 \pmod 4$ wird.

Wenn wir dann in der Gleichung (19)

$$(25) \qquad v_1 = f_2\left(\frac{\omega}{2}\right)^3 = \frac{\sqrt{2}^3}{f_1(\omega)^3}, \quad u_1 = f_1(\omega)^3$$

setzen, so ergibt sich eine Gleichung, die nur $\sqrt{2}\,f_1(\omega)^6$ und rationale Koeffizienten enthält. (19) ist aber nur dann erfüllt [§ 40, (7)], wenn

(26) $$\frac{c + \partial\omega}{a} = \frac{2\gamma + \delta\omega}{2\alpha + \beta\omega}, \quad \delta \equiv 0 \pmod 2$$

und außerdem

(27) $$\gamma^2 - 1 + \gamma(2\alpha - \delta) \equiv 0 \pmod{16};$$

aus (26) und (24) folgt:

$$\begin{matrix} 2\alpha = B + y, & 2n\gamma \equiv -C \\ \beta = A, & 2n\delta \equiv -(B-y) \end{matrix} \pmod{16},$$

und daraus schließt man wie oben:

9. Ist $m \equiv 2 \pmod 4$, so ist $\sqrt{2}\, f_1(\omega)^6$ Klasseninvariante.

Wiederum weisen sämtliche Beispiele darauf hin, daß, wenn $m \equiv 4 \pmod 8$ ist, $\sqrt{2}\, f_1(\omega)^{12}$ Klasseninvariante ist. Aber auch hierfür fehlt noch der Beweis. Wenn m durch 8 teilbar ist, tritt eine Reduktion nicht ein.

In den Fällen 4. bis 8. ergibt sich nach 3. eine weitere Reduktion auf die dritte Wurzel, wenn m nicht durch 3 teilbar ist. Demnach erhalten wir folgende Fälle:

$$m \equiv \pm 1 \pmod 3,$$

		Klasseninvariante
1)	$m \equiv 3 \pmod 4$	$f(\omega)^2$,
2)	$m \equiv 5 \pmod 8$	$f(\omega)^4$,
3)	$m \equiv 1$ „	$\sqrt{2}\, f(\omega)^2$,
4)	$m \equiv 7$ „	$\sqrt{2}\, f(\omega)$,
5)	$m \equiv 3$ „	$f(\omega)$,
6)	$m \equiv 2$ „	$\sqrt{2}\, f_1(\omega)^2$,
7)	$m \equiv 4$ „	$\sqrt{2}\, f_1(\omega)^4$,

wovon freilich die Fälle 5) und 7) nur durch Induktion geschlossen sind.

Die Klasseninvarianten $f(\omega)$ eignen sich ganz besonders zur numerischen Berechnung, weil sie unter allen die einfachsten Resultate liefern. Wir geben daher zunächst eine größere Reihe von Beispielen, die sich auf Grund unserer bisherigen Entwickelungen leicht ableiten lassen, und die zugleich die Methoden kennen lehren, deren man sich auch zu weiter fortgesetzten Rechnungen dieser Art bedienen kann.

Es wird bei diesen Berechnungen häufig die Aufgabe gestellt, reduzible, ganze rationale Funktionen in Faktoren zu zerlegen. Eine solche Zerlegung ist, wenn sie gefunden ist, natürlich sofort

zu verifizieren; aber auch das Auffinden der Faktoren gelingt leicht, wenigstens soweit die Rechnungen bis jetzt fortgesetzt sind, da man häufig in den späteren Fällen früher gefundene Resultate benutzen kann, und überdies die allgemeine Form der Faktoren kennt. Beispiele werden dies erläutern.

§ 128. Die ersten Fälle der Berechnung von $f(\sqrt{-m})$.

Setzen wir in der kubischen Gleichung:

(1) $$u^3 - \gamma_2(\omega)u - 16 = 0,$$

deren Wurzeln nach § 54

$$f(\omega)^8, \quad -f_1(\omega)^8, \quad -f_2(\omega)^8$$

sind, $\omega = i$, also [§ 125, (16)], $\gamma_2 = 12$, so folgt:

$$u^3 - 12u - 16 = 0,$$

eine Gleichung, deren einzige positive Wurzel $u = 4$ ist, so daß wir in Übereinstimmung mit § 126 erhalten:

(2) $$f(i) = \sqrt[4]{2};$$

setzen wir $\omega = \sqrt{-2}$, also $\gamma_2 = 20$ [§ 125, (17)], so erhalten wir aus (1) die Gleichung:

$$u^3 - 20u - 16 = 0$$

mit der einzigen rationalen Wurzel -4. Da aber nach den Sätzen der beiden vorhergehenden Paragraphen $f_1(\sqrt{-2})^8$ rational sein muß, so ist:

(3) $$f_1(\sqrt{-2}) = \sqrt[4]{2}.$$

Wir setzen ferner $\omega = e^{\frac{2\pi i}{3}}$, also $\gamma_2(\omega) = 0$ (§ 117) und erhalten aus (1):

$$u^3 = 16.$$

Dieser Gleichung genügt [§ 34, (19)]:

$$u = -f_2\left(\frac{-1+\sqrt{-3}}{2}\right)^8 = \frac{16\, e^{\frac{2\pi i}{3}}}{f(\sqrt{-3})^8},$$

woraus der reelle positive Wert:

(4) $$f(\sqrt{-3}) = \sqrt[3]{2}.$$

Um die übrigen Resultate des § 125 anwenden zu können, setzen wir

$$m = 7, \quad 11, \quad 19, \quad 43, \quad 67, \quad 163,$$

und benutzen die aus § 34, (19) folgende Formel:

$$f(\omega) f_2\left(\frac{-3+\omega}{2}\right) = e^{-\frac{\pi i}{8}}\sqrt{2}.$$

Demnach ist, wenn wir

$$f(\sqrt{-m}) = x$$

setzen, x nach (1) die reelle positive Wurzel der Gleichung

(5) $$x^{24} + \gamma_2\left(\frac{-3+\sqrt{-m}}{2}\right) x^{16} - 2^8 = 0.$$

Für $m = 7$ erhalten wir nach § 125, (18)

(6) $$f(\sqrt{-7}) = \sqrt{2},$$

während in den anderen Fällen, nach Einsetzen der Werte für γ_2, sich die Gleichung (5) erst in zwei Faktoren 12ten, diese wieder in zwei Faktoren 6ten und schließlich diese in zwei 3ten Grades spaltet. Die so erhaltenen Gleichungen sind kubische Gleichungen für x^8, x^4, x^2, x, von denen wir jedesmal nur die beibehalten, die eine reelle positive Wurzel hat, der schließlich $f(\sqrt{-m})$ selbst genügt.

Um die erste Zerlegung zu finden, setzen wir die Gleichung (5) in die Form:

$$(x^{12} - a x^4)^2 - (b x^8 + c)^2 = 0,$$

und haben die ganzen Zahlen a, b, c aus den Gleichungen:

$$2a + b^2 = -\gamma_2, \quad 2bc = a^2, \quad c^2 = 2^8$$

zu bestimmen, also $c = \pm 16$; die Gleichung 12ten Grades mit positiver Wurzel lautet also:

$$x^{12} - b x^8 - a x^4 - 16 = 0.$$

Die Zahlen a, b bestimmen sich aus den obigen Gleichungen leicht, und so findet man schließlich die gesuchten kubischen Gleichungen. Man erhält z. B. für $m = 11$ successive

$$x^{12} - 8x^8 + 16x^4 - 16 = 0,$$
$$x^6 - 4x^2 - 4 = 0,$$
$$x^3 - 2x^2 + 2x - 2 = 0.$$

In den fünf Fällen des § 125 findet man folgende Gleichungen:

(7) $$x = f(\sqrt{-11}), \quad x^3 - 2x^2 + 2x - 2 = 0,$$
(8) $$x = f(\sqrt{-19}), \quad x^3 - 2x - 2 = 0,$$
(9) $$x = f(\sqrt{-43}), \quad x^3 - 2x^2 - 2 = 0,$$
(10) $$x = f(\sqrt{-67}), \quad x^3 - 2x^2 - 2x - 2 = 0,$$
(11) $$x = f(\sqrt{-163}), \quad x^3 - 6x^2 + 4x - 2 = 0.$$

§ 129. Anwendung der Transformation zweiter Ordnung zur Berechnung von Klasseninvarianten.

Die Transformation zweiter Ordnung läßt sich, wenn nötig in mehrmaliger Wiederholung, auf alle solche Diskriminanten $-4m$ anwenden, für die $y^2 + mx^2$ eine Potenz von 2 ist, also z. B. auf $m = 7, 15, 23, 31$.

Diese Rechnungen sind aber beschwerlich, und wir werden einfachere Wege finden, um in diesen Fällen zum Ziele zu kommen. Bessere Dienste leistet die Transformation zweiter Ordnung, um aus einer bekannten Klasseninvariante eine neue zu finden, die zu einer Diskriminante gehört, die das Vierfache der ersteren ist.

Dazu führen folgende Formeln:

Nach § 34 ist:

$$f_1(\omega)^8 + f_2(\omega)^8 = f(\omega)^8,$$

$$f_1(\omega)^8 f_2(\omega)^8 = \frac{16}{f(\omega)^8},$$

woraus

$$f_1(\omega)^8 - f_2(\omega)^8 = \frac{\sqrt{f(\omega)^{24} - 64}}{f(\omega)^4}.$$

Das Vorzeichen der Wurzel wechselt nur für $f(\omega)^{24} = 64$, also für $\omega = i$, und ist, solange $-i\omega$ reell und größer als 1 ist, positiv zu nehmen, da die linke Seite für ein verschwindendes q positiv unendlich wird. Es ergibt sich daraus:

$$2 f_2(\omega)^8 = \frac{f(\omega)^{12} - \sqrt{f(\omega)^{24} - 64}}{f(\omega)^4},$$

oder

$$f_2(\omega)^8 f(\omega)^4 \left[f(\omega)^{12} + \sqrt{f(\omega)^{24} - 64}\right] = 32,$$

und auf dieselbe Weise:

$$f_2(\omega)^8 f_1(\omega)^4 \left[f_1(\omega)^{12} + \sqrt{f_1(\omega)^{24} + 64}\right] = 32.$$

Ferner ist nach § 34, (16):

$$f_1(2\omega) f_2(\omega) = \sqrt{2},$$

woraus

(1) $$2 f_1(2\omega)^8 = f(\omega)^4 \left[f(\omega)^{12} + \sqrt{f(\omega)^{24} - 64}\right],$$
$$= f_1(\omega)^4 \left[f_1(\omega)^{12} + \sqrt{f_1(\omega)^{24} + 64}\right].$$

Diese Formeln können dazu dienen, wenn $f(\omega)$ oder $f_1(\omega)$ bekannt ist, $f_1(2\omega)$ zu berechnen, also $f_1(\sqrt{-4m})$ aus $f(\sqrt{-m})$

oder $f_1(\sqrt{-m})$. Auf diese Weise findet man sehr leicht, wenn man aus den Formeln des vorigen Paragraphen $f(i)$, $f_1(\sqrt{-2})$, $f(\sqrt{-3})$, $f(\sqrt{-7})$ entnimmt:

(2) $f_1(\sqrt{-4})^8 = 8,$

(3) $f_1(\sqrt{-16})^8 = 8\sqrt{2}(1+\sqrt{2})^2,$

(4) $f_1(\sqrt{-8})^8 = 8(1+\sqrt{2}),$

(5) $f_1(\sqrt{-32})^8 = 32(1+\sqrt{2})^2 + 8\sqrt{2}\sqrt{8(1+\sqrt{2})^4+(1+\sqrt{2})}.$

Setzen wir:

$$f_1(\sqrt{-32})^8 = 8x,$$

so ist x Wurzel der biquadratischen Klassengleichung:

(6) $$(x^2 - 24x - 2)^2 - 8(8x+1)^2 = 0,$$

die durch Adjunktion von $\sqrt{2}$ in zwei quadratische Gleichungen

$$x^2 - 8(1 \pm \sqrt{2})^2 x - 2(1 \pm \sqrt{2}) = 0$$

zerfällt. Ferner finden wir so:

(7) $$f_1(\sqrt{-12})^4 = 2\sqrt[6]{2}(1+\sqrt{3}),$$

(8) $$f_1(\sqrt{-28})^4 = 2\sqrt{2}(3+\sqrt{7}).$$

Auf andere Fälle werden wir diese Methode später noch anwenden.

§ 130. Berechnung von Klasseninvarianten aus den Schlaeflischen Modulargleichungen.

I. Wenn wir in einer der Gleichungen zwischen $u = f(\omega)$ und $v = f(n\omega)$ oder zwischen $u = f_1(\omega)$, $v = f_1(n\omega)$ (§ 73), für u einen der bekannten Werte von $f(\sqrt{-m})$ oder $f_1(\sqrt{-m})$ einsetzen, so erhalten wir eine Gleichung, welcher $f(\sqrt{-n^2m})$ oder $f_1(\sqrt{-n^2m})$ genügt.

Diese Gleichung enthält unter Umständen noch fremde Faktoren, die man aufzusuchen und zu beseitigen hat.

Ist n eine Primzahl, so erhalten wir nach § 123 vollständigen Aufschluß über diese überflüssigen Faktoren. Geht n in m auf, so ist in der betreffenden Gleichung ein zur Determinante $-m$ gehöriger Linearfaktor abzusondern, ist $-m$ quadratischer Nichtrest von n, so sind überflüssige Faktoren überhaupt nicht vorhanden, ist $-m$ quadratischer Rest von n, so ist ein zur Diskri-

minante $-4m$ gehöriger quadratischer Faktor abzusondern, und wenn $m = 1$ ist, so ist die nach Absonderung der fremden Faktoren übrig bleibende Gleichung ein Quadrat.

Als Beispiele für diese Fälle nehmen wir:

1. $m = 3, \quad n = 3,$ Absonderung eines Linearfaktors.
2. $m = 2, \quad n = 5,$ kein fremder Faktor.
3. $m = 2, \quad n = 3,$ Absonderung eines quadratischen Faktors.
4. $m = 1, \quad n = 3,$ Quadrat.
5. $m = 1, \quad n = 5,$ Quadrat nach Absonderung eines quadratischen Faktors.
6. $m = 1, \quad n = 7,$ Quadrat.

Im Falle 1. hat man in der auf den Transformationsgrad $n = 3$ bezüglichen Formel des § 73 zu setzen:

$$u^3 = 2, \quad v^3 = f(\sqrt{-27})^3 = 2x,$$

also

$$A = x^2 + \frac{1}{x^2}, \quad B = 4x - \frac{2}{x},$$

und folglich:

$$x^4 - 4x^3 + 2x + 1 = (x - 1)(x^3 - 3x^2 - 3x - 1) = 0,$$

so daß man für $m = 27$ erhält:

$$(1) \qquad f(\sqrt{-27})^3 = 2x, \quad x^3 - 3x^2 - 3x - 1 = 0.$$

Im Falle 2. setzen wir im System II. des § 73 $(n = 5)$:

$$u_1 = f_1(\sqrt{-2}) = \sqrt[4]{2}, \quad v_1 = f_1(\sqrt{-50}) = \sqrt[4]{2}\,x,$$

$$A_1 = \frac{1}{x^3} - x^3, \qquad B_1 = 2\left(x^2 + \frac{1}{x^2}\right),$$

so daß man (ohne fremden Teiler) die Gleichung 6ten Grades:

$$(2) \qquad \frac{1}{x^3} - x^3 + 2\left(x^2 + \frac{1}{x^2}\right) = 0, \quad f_1(\sqrt{-50}) = \sqrt[4]{2}\,x$$

erhält, die sich für

$$y = \frac{1}{x} - x$$

auf den dritten Grad reduziert:

$$(3) \qquad y^3 + 2y^2 + 3y + 4 = 0.$$

Im Falle 3. setzen wir im System II. des § 73 ($n = 3$):

$$u_1 = \sqrt[4]{2}, \quad v_1^3 = f_1(\sqrt{-18})^3 = \sqrt[4]{2}\,x,$$

$$A_1 = \frac{2}{x^2} - \frac{x^2}{2}, \quad B_1 = 2x + \frac{4}{x},$$

$$x^4 - 4x^3 - 8x - 4 = (x^2 + 2)(x^2 - 4x - 2),$$

also

(4) $$x^2 - 4x - 2 = 0, \quad f_1(\sqrt{-18})^3 = \sqrt[4]{2}\,x.$$

Die Auflösung von (4) ergibt:

(5) $$x = 2 + \sqrt{6}.$$

Im Falle 4. ist:

$$u = f(i) = \sqrt[4]{2}, \quad v^3 = f(\sqrt{-9})^3 = \sqrt[4]{2}\,x,$$

$$A = \frac{x^2}{2} + \frac{2}{x^2}, \quad B = 2x - \frac{4}{x},$$

$$x^4 - 4x^3 + 8x + 4 = (x^2 - 2x - 2)^2 = 0,$$

also

(6) $$x^2 - 2x - 2 = 0, \quad f(\sqrt{-9})^3 = \sqrt[4]{2}\,x,$$

(7) $$x = 1 + \sqrt{3}.$$

Im Falle 5.:

$$u = f(i) = \sqrt[4]{2}, \quad v = f(\sqrt{-25}) = \sqrt[4]{2}\,x,$$

$$A = x^3 + \frac{1}{x^3}, \quad B = 2\left(x^2 - \frac{1}{x^2}\right),$$

$$x^3 + \frac{1}{x^3} - 2\left(x^2 - \frac{1}{x^2}\right) = \left(x + \frac{1}{x}\right)\left(x - \frac{1}{x} - 1\right)^2 = 0.$$

(8) $$x - \frac{1}{x} - 1 = 0, \quad f(\sqrt{-25}) = \sqrt[4]{2}\,x,$$

(9) $$x = \frac{1 + \sqrt{5}}{2}.$$

Endlich setzen wir für $n = 7$:

$$u = \sqrt[4]{2}, \quad v = f(\sqrt{-49}) = \frac{x}{\sqrt[4]{2}}$$

und finden

$$\begin{aligned} 0 &= (x^8 - 4x^7 + 28x^4 - 32x + 16) \\ &= (x^4 - 2x^3 - 2x^2 - 4x + 4)^2, \end{aligned}$$

woraus leicht durch Auflösung einer quadratischen Gleichung:

(10) $$x + \frac{2}{x} = 1 + \sqrt{7}, \quad x = \sqrt[4]{2}\,f(\sqrt{-49}).$$

Auf dieselbe Weise sind die in der Tabelle am Ende aufgeführten Klasseninvarianten für

$$m = 75, \quad 36, \quad 100, \quad 63, \quad 175$$

berechnet, und diese Rechnungen lassen sich auch noch weiter fortsetzen.

II. Aus den Schlaeflischen Modulargleichungen läßt sich noch auf verschiedene andere Arten für die Berechnung von Klasseninvarianten Nutzen ziehen.

Setzen wir

$$\omega = -\frac{m}{\omega}, \quad \omega = \sqrt{-m},$$

so wird

$$f(\omega) = f\left(\frac{\omega}{m}\right) = f(\sqrt{-m}); \tag{11}$$

wenn also in der Modulargleichung für den Transformationsgrad m

$$u = v$$

gesetzt wird, so ergibt sich eine Gleichung, unter deren Wurzeln $u = f(\sqrt{-m})$ vorkommt. In dem System I. des § 73 ist dann immer $A = 2$ zu setzen, und es ergeben sich die Formeln:

$$m = 3, \quad B = u^6 - \frac{8}{u^6} = 2,$$

$$m = 5, \quad B = u^4 - \frac{4}{u^4} = 2,$$

$$m = 7, \quad B = u^6 + \frac{8}{u^6} = 9,$$

$$m = 11, \quad B = u^2 - \frac{2}{u^2}, \quad B^5 - B^3 - 2B = 2,$$

$$m = 13, \quad B = u^{12} - \frac{64}{u^{12}} = 9 \cdot 2^5,$$

$$m = 17, \quad B = u^8 + \frac{16}{u^8}, \quad B^2 - 68B - 544 = 0,$$

$$m = 19, \quad B = u^6 - \frac{8}{u^6}, \quad B^3 - 38B^2 + 252B - 648 = 0.$$

Die Fälle $m = 3, 7, 11, 19$ ergeben keine neuen Resultate, können aber zur Verifizierung der früher gefundenen verwandt werden; aus $m = 5, 13$ erhalten wir durch Auflösung einer quadratischen Gleichung:

(12) $$f(\sqrt{-5})^4 = 1 + \sqrt{5},$$

(13) $$f(\sqrt{-13})^4 = 3 + \sqrt{13}.$$

Für $m = 17$ ist die Klassenzahl 4, also die oben angegebene Gleichung, die in bezug auf u^8 vom 4ten Grade ist, die Klassengleichung. Löst man sie in bezug auf B auf, so erhält man:

$$u^8 + \frac{16}{u^8} = 34 + 10\sqrt{17},$$

$$u^4 + \frac{4}{u^4} = 5 + \sqrt{17},$$

$$\left(u^2 + \frac{2}{u^2}\right)^2 = \frac{(1 + \sqrt{17})^2}{2}.$$

Wenn man also

$$\sqrt{2}x = f(\sqrt{-17})^2$$

setzt, so erhält man für x die quadratische Gleichung:

(14) $$x + \frac{1}{x} = \frac{1 + \sqrt{17}}{2}.$$

III. Wir setzen für ω die Wurzel der quadratischen Gleichung:

$$2\omega^2 + 2r\omega + n = 0,$$

worin n eine ungerade ganze Zahl bedeutet und r eine ganze Zahl, deren Quadrat kleiner als $2n$ ist, also:

(15) $$2\omega + 2r = -\frac{n}{\omega},$$

(16) $$\omega = \frac{-r + \sqrt{-m}}{2}, \quad m = 2n - r^2.$$

Es ist dann nach § 34:

(17) $$f_2(\omega) f_1(2\omega + 2r) = e^{-\frac{r\pi i}{12}} \sqrt{2},$$

und nach (15), (16):

(18) $$f_2(\omega) f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{12}} \sqrt{2},$$

(19) $$f_2(\omega) = \frac{e^{-\frac{r\pi i}{12}} \sqrt{2}}{f_1(r + \sqrt{-m})};$$

setzen wir also, je nachdem r und folglich auch m gerade oder ungerade ist,

(20) $$x = f_1(\sqrt{-m}), \quad x = f(\sqrt{-m}),$$

so wird

(21) $$f_2(\omega) = \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x}, \quad f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}} x,$$

und diese Werte hat man für u_1, v_1 in das System II., § 73 zu substituieren, um eine Gleichung für x zu erhalten.

Indem man für r die verschiedenen zulässigen Werte setzt, bekommt man aus (16):

$$\begin{aligned}
n &= 3, & m &= 6,\ 5,\ 2,\\
n &= 5, & m &= 10,\ 9,\ 6,\ 1,\\
n &= 7, & m &= 14,\ 13,\ 10,\ 5,\\
n &= 11, & m &= 22,\ 21,\ 18,\ 13,\ 6,\\
n &= 13, & m &= 26,\ 25,\ 22,\ 17,\ 10,\ 1,\\
n &= 17, & m &= 34,\ 33,\ 30,\ 25,\ 18,\ 9,\\
n &= 19, & m &= 38,\ 37,\ 34,\ 29,\ 22,\ 13,\ 2.
\end{aligned}$$

Als einfaches Beispiel wählen wir $n = 7$ und erhalten aus § 73, II.:

$$\frac{x^8}{4} + \frac{4}{x^8} = 7 + 4\sqrt{2}\cos\frac{r\pi}{4}.$$

Daraus ergibt sich für $r = 0$:

(22) $$\frac{x^2}{\sqrt{2}} + \frac{\sqrt{2}}{x^2} = 1 + \sqrt{2}, \quad x = f_1(\sqrt{-14}),$$

für $r = 1$ das bereits bekannte

(23) $$f(\sqrt{-13})^4 = 3 + \sqrt{13},$$

für $r = 2$:

(24) $$f_1(\sqrt{-10})^2 = \frac{1+\sqrt{5}}{\sqrt{2}}.$$

Als zweites Beispiel nehmen wir noch $n = 13$ und erhalten:

(25) $$A_1 = \frac{\sqrt{2}}{x^2} - \frac{x^2}{\sqrt{2}}, \quad B_1 = 16\cos\frac{r\pi}{2};$$

für $r = 0, 4$, also $m = 26, 10$ ergibt sich hieraus $B_1 = 16$, und folglich nach § 73:

$$A_1^7 - 6A_1^5 + A_1^3 + 20A_1 + 16 = 0,$$

während für $r = 2$, also $m = 22$ in dieser Gleichung A_1 in $-A_1$ zu verwandeln ist.

Man findet aber leicht die Zerlegung:

(26) $$\begin{aligned} &A_1^7 - 6A_1^5 + A_1^3 + 20A_1 + 16\\ &= (A_1+1)^2(A_1-2)^2(A_1^3 + 2A_1^2 + A_1 + 4).\end{aligned}$$

Ist $-i\omega > \sqrt{2}$, so ist auch $f_1^2(\omega) > \sqrt{2}$, denn $f_1(\omega)^2$ geht, während $-i\omega$ von $\sqrt{2}$ bis ∞ geht, ebenfalls, und zwar stets wachsend[1]), von $\sqrt{2}$ bis ∞, und folglich ist A_1 negativ für $r = 0, 2, 4$.

Der erste Faktor $A_1 + 1$ verschwindet, wie aus dem schon bekannten Resultat (24) hervorgeht, für $r = 4$; daher verschwindet der dritte Faktor $A_1^3 + 2A_1^2 + A_1 + 4$ für $r = 0$, während $A_1 + 2$ für $r = 2$ verschwindet.

Wir erhalten also nach (25):

$$(27) \quad f_1(\sqrt{-10})^2 = \sqrt{2}\,y, \quad y - \frac{1}{y} = 1,$$

$$(28) \quad f_1(\sqrt{-22})^2 = \sqrt{2}\,y, \quad y - \frac{1}{y} = 2,$$

$$(29) \quad f_1(\sqrt{-26})^2 = \sqrt{2}\,y, \; y^6 - 2y^5 - 2y^4 + 2y^2 - 2y - 1 = 0.$$

IV. Als Beispiel für eine andere Art der Verwendung der Schlaeflischen Modulargleichungen, die zu der sonst schwer zugänglichen Klasseninvariante $f(\sqrt{-41})$ führt, möge das Folgende dienen.

Wir setzen:

$$(30) \qquad 2n\omega^2 + 2r\omega + n = 0,$$

$$(31) \qquad \omega = \frac{-r + \sqrt{-m}}{2n}, \quad m = 2n^2 - r^2.$$

Es kann hierin r jede Zahl bedeuten, die m positiv macht, die aber mit n keinen Teiler gemeinschaftlich hat [weil sonst (30) imprimitiv ist]. Es wird dann nach § 34:

$$(32) \qquad f_2\left(\frac{\omega}{n}\right) = f_1[2(n\omega + r)] = \frac{e^{-\frac{r\pi i}{12}}\sqrt{2}}{f_2(n\omega)},$$

$$f_1[2(n\omega + r)] = f_1(r + \sqrt{-m}) = e^{-\frac{r\pi i}{24}}\,x,$$

---

[1]) Aus § 54, (11) folgt nämlich durch die Substitution $\left(\omega, 1 - \frac{1}{\omega}\right)$:

$$d f_1(\omega)^8 = -\frac{\pi i}{3}\,\vartheta_{10}^4\,[f(\omega)^8 + f_1(\omega)^8]\,d\omega.$$

also:

$$f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}} x,$$

$$f_2(n\omega) = \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x},$$

wenn, je nachdem r gerade oder ungerade ist,

(33) $$x = f_1(\sqrt{-m}) \quad \text{oder} \quad = f(\sqrt{-m})$$

gesetzt wird. Nehmen wir also in der zu n gehörigen Modulargleichung II., § 73:

$$u_1 = f_2(\omega),$$

$$v_1 = \left(\frac{2}{n}\right) f_2(n\omega) = \left(\frac{2}{n}\right) \frac{e^{-\frac{r\pi i}{24}}\sqrt{2}}{x}$$

oder

$$v_1 = f_2\left(\frac{\omega}{n}\right) = e^{-\frac{r\pi i}{24}} x,$$

so ergeben sich zwei Gleichungen, aus denen man durch Elimination von u_1 eine Gleichung für x herleitet.

Um für $n = 5$ diese Rechnung durchzuführen, setzen wir:

(34) $$x f_2(\omega) = \sqrt{2}\, e^{-\frac{5r\pi i}{24}} \xi, \qquad \frac{x}{f_2(\omega)} = e^{-\frac{5r\pi i}{24}} \eta,$$

woraus man, entsprechend den beiden Annahmen für v_1, für ein ungerades r die Gleichungen erhält:

(35) $$\xi^3 + \frac{1}{\xi^3} + 2\left(\eta^2 - \frac{1}{\eta^2}\right) = 0, \qquad \eta^3 + \frac{1}{\eta^3} + 2\left(\xi^2 - \frac{1}{\xi^2}\right) = 0.$$

Diese Gleichungen gelten für $r = 1, 3, 7$, die zu den Werten $m = 49, 41, 1$ gehören.

Subtrahiert man die beiden Gleichungen (35), so kann man den Faktor $\xi - \eta$ abwerfen, der nur für $m = 1$ verschwinden kann:

$$[(\xi + \eta)^2 - \xi\eta]\left(1 - \frac{1}{\xi^3\eta^3}\right) - 2(\xi + \eta)\left(1 + \frac{1}{\xi^2\eta^2}\right) = 0,$$

und wenn man die beiden Gleichungen (35) addiert:

$$[(\xi+\eta)^3 - 3\xi\eta(\xi+\eta)]\left(1+\frac{1}{\xi^3\eta^3}\right)$$
$$+ 2[(\xi+\eta)^2 - 2\xi\eta]\left(1-\frac{1}{\xi^2\eta^2}\right) = 0.$$

Es ist aber nach (34):

$$\sqrt{2}\,\xi\eta = x^2,$$

und man erhält also eine Gleichung für x^2, wenn man $(\xi+\eta)$ eliminiert. Diese Gleichung wird nach dem gewöhnlichen Eliminationsverfahren, wenn man

$$z = \frac{x^2}{\sqrt{2}} + \frac{\sqrt{2}}{x^2}$$

setzt, in der Form

$$(36)\qquad z^6 - 9z^5 + 20z^4 + 6z^3 - 19z^2 - 17z - 6 = 0$$

gefunden. Hierin ist aber noch der auf die Determinante -49 bezügliche Faktor enthalten. Für diesen ist [nach Formel (10)]:

$$z = 2 + \sqrt{7}.$$

Es muß also die linke Seite von (36) durch

$$z^2 - 4z - 3$$

teilbar sein, und die Ausführung der Division ergibt den für die Determinante -41 gültigen Faktor:

$$(37)\qquad \begin{aligned} &z^4 - 5z^3 + 3z^2 + 3z + 2 = 0,\\ &z = \frac{f(\sqrt{-41})}{\sqrt{2}} + \frac{\sqrt{2}}{f(\sqrt{-41})}. \end{aligned}$$

§ 131. Berechnung von Klasseninvarianten aus den irrationalen Formen der Modulargleichungen.

In außerordentlich einfacher Weise führen vielfach die irrationalen Formen der Modulargleichungen zur Aufstellung von Klassengleichungen.

1. Im § 75 haben wir gesehen, daß, falls $m \equiv -1 \pmod 8$ ist, zwischen den beiden Funktionen:

$$2A = f(\omega)f(m\omega) + (-1)^{\frac{m+1}{8}}[f_1(\omega)f_1(m\omega) + f_2(\omega)f_2(m\omega)],$$

$$B = \frac{2}{f_1(\omega)f_1(m\omega)} + \frac{2}{f_2(\omega)f_2(m\omega)} + \frac{(-1)^{\frac{m+1}{8}}\,2}{f(\omega)f(m\omega)}$$

eine algebraische Gleichung besteht, und diese Gleichungen sind dort für $m = 7, 23, 31, 47, 71$ aufgestellt.

Setzen wir darin:

$$\omega = \frac{-1}{\sqrt{-m}}, \quad m\omega = \sqrt{-m}, \quad f(\sqrt{-m}) = \sqrt{2}\, x,$$

so wird nach § 34:

$$A = x^2 + \frac{(-1)^{\frac{m+1}{8}}}{x}, \quad B = 4x + \frac{(-1)^{\frac{m+1}{8}}}{x}.$$

Daraus ergibt sich z. B. für $m = 23$, wo $A = 1$ ist, die Gleichung:

(1) $$f(\sqrt{-23}) = \sqrt{2}\, x, \quad x^3 - x - 1 = 0$$

und für $m = 31$:

$$x^9 - 4x^6 + 3x^3 - 1 = 0.$$

Dies ist zunächst eine kubische Gleichung für x^3; man spaltet daraus aber leicht die kubische Gleichung für x selbst ab:

(2) $$f(\sqrt{-31}) = \sqrt{2}\, x, \quad x^3 - x^2 - 1 = 0.$$

Ähnlich ergeben sich die Gleichungen:

(3) $$f(\sqrt{-47}) = \sqrt{2}\, x,$$
$$x^5 - x^3 - 2x^2 - 2x - 1 = 0,$$

(4) $$f(\sqrt{-71}) = \sqrt{2}\, x,$$
$$x^7 - 2x^6 - x^5 + x^4 + x^3 + x^2 - x - 1 = 0.$$

Im letzten Falle, $m = 71$, ist von der unmittelbar erhaltenen Gleichung 9ten Grades der der Aufgabe fremde Faktor $(x + 1)^2$ abgesondert.

2. Um zu einer weiteren Berechnungsart zu gelangen, wenden wir die Transformation zweiter Ordnung an. Wir haben zunächst allgemein [für ein veränderliches ω, § 34, (17)]:

$$f(2\omega)^8 + f_2(2\omega)^8 = 2\,\frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4},$$

$$f(2\omega)^8 - f_2(2\omega)^8 = \frac{16}{f_2(\omega)^8},$$

woraus:

$$f(2\omega)^8 = \frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4} + \frac{8}{f_2(\omega)^8},$$

$$f_2(2\omega)^8 = \frac{f(\omega)^8 + f_1(\omega)^8}{f_2(\omega)^4} - \frac{8}{f_2(\omega)^8};$$

daraus

$$f(\omega)^8 f(2\omega)^8 + f_1(\omega)^8 f_2(2\omega)^8 = 8 + \frac{[f(\omega)^8 + f_1(\omega)^8]^2}{f_2(\omega)^4},$$

was sich nach § 34 leicht in die Form bringen läßt:

$$[f(\omega)^4 f(2\omega)^4 + f_1(\omega)^4 f_2(2\omega)^4]^2 = 16 + f_2(\omega)^{12} + \frac{64}{f_2(\omega)^{12}},$$

und hieraus kann die Wurzel gezogen werden:

(5) $$f(\omega)^4 f(2\omega)^4 + f_1(\omega)^4 f_2(2\omega)^4 = f_2(\omega)^6 + \frac{8}{f_2(\omega)^6}.$$

Es genüge nun ω der quadratischen Gleichung:

(6) $$2\omega^2 + 2r\omega + n = 0$$

mit ungeradem n, also:

(7) $$\omega = \frac{-r + \sqrt{-m}}{2}, \quad m = 2n - r^2.$$

Wenn dann

(8) $$\sqrt{2}\, x = f(\sqrt{-m})^2, \quad \text{oder} \quad = f_1(\sqrt{-m})^2$$

gesetzt wird, je nachdem r ungerade oder gerade ist, so wird

(9) $$f_2(\omega)^2 = e^{-\frac{r\pi i}{12}} \frac{\sqrt{2}}{x}.$$

Ferner folgt aus

$$2\omega = -\frac{n}{\omega} - 2r$$

nach den Formeln des § 34:

(10) $$\begin{aligned} f(2\omega) &= f\left(\frac{\omega}{n}\right) e^{\frac{r\pi i}{12}} \\ f_1(2\omega) &= f_2\left(\frac{\omega}{n}\right) e^{\frac{r\pi i}{12}} \\ f_2(2\omega) &= f_1\left(\frac{\omega}{n}\right) e^{-\frac{r\pi i}{6}}, \end{aligned}$$

so daß die Gleichung (5) ergibt:

(11) $$f(\omega)^4 f\left(\frac{\omega}{n}\right)^4 + (-1)^r f_1(\omega)^4 f_1\left(\frac{\omega}{n}\right)^4 = e^{-\frac{r\pi i}{12}} \sqrt{8}\left(x^3 + \frac{e^{-\frac{r\pi i}{2}}}{x^3}\right).$$

Aus (10) folgt noch weiter:

$$(12) \qquad f_2(\omega) f_2\left(\frac{\omega}{n}\right) = \sqrt{2}\, e^{-\frac{r\pi i}{12}},$$

$$(13) \qquad f(\omega) f\left(\frac{\omega}{n}\right) f_1(\omega) f_1\left(\frac{\omega}{n}\right) = \sqrt{2}\, e^{\frac{r\pi i}{12}}.$$

Wenn wir $n = 23$ und $r = 0$ annehmen, so gibt die Gleichung § 75, (8) mit Benutzung von (12):

$$(14) \qquad f(\omega) f\left(\frac{\omega}{n}\right) - f_1(\omega) f_1\left(\frac{\omega}{n}\right) = 2 + \sqrt{2},$$

woraus durch zweimaliges Quadrieren mit Benutzung von (11) und (13) folgt:

$$x^3 + \frac{1}{x^3} = 36 + 26\sqrt{2};$$

hieraus leitet man die einfachere Gleichung ab:

$$(15) \qquad x + \frac{1}{x} = 3 + \sqrt{2}, \quad \sqrt{2}\, x = f_1^2(\sqrt{-46}).$$

3. Wir machen endlich noch eine Anwendung der Transformationsgleichungen des § 76 für einen zusammengesetzten Transformationsgrad auf die Determinante -39.

Setzen wir

$$u = f(\sqrt{-39}), \quad v = f\left(\sqrt{\frac{-13}{3}}\right), \quad \frac{u^2 + v^2}{uv} = z,$$

so ist in der auf $n = 39$ bezüglichen Gleichung (22), § 76 zu setzen:

$$A = \frac{u^2}{v^2} - 2\frac{v}{u}, \quad B = \frac{v^2}{u^2} - 2\frac{u}{v},$$

und die erwähnte Gleichung gibt:

$$z^3 + z^2 - 5z - 6 = 0,$$

woraus nach Abwerfung des Faktors $z + 2$ die folgende hervorgeht:

$$(16) \qquad z^2 - z - 3 = 0, \quad z = \frac{1 + \sqrt{13}}{2}.$$

Zwischen u und v besteht aber andererseits eine Transformationsgleichung dritter Ordnung (§ 73):

$$\frac{u^6 v^6 - 8}{u^3 v^3} = \frac{u^{12} + v^{12}}{u^6 v^6} = z^6 - 6z^4 + 9z^2 - 2,$$

was sich mit Hilfe von (16) auf die Form $z^4 - 2 = \frac{27 + 7\sqrt{13}}{2}$ bringen läßt.

Daraus erhält man

$$u^3 v^3 = 4\,(3 + \sqrt{13}),$$
$$u^6 + v^6 = 4\,(17 + 5\,\sqrt{13}),$$
$$u^3 - v^3 = \sqrt{2}\,(3 + \sqrt{13}),$$

so daß, wenn $u^3 = \sqrt{8}\,x$ gesetzt wird, für x die quadratische Gleichung folgt:

$$(17) \qquad x^2 - \frac{3 + \sqrt{13}}{2}\,(x + 1) = 0, \quad f(\sqrt{-39})^3 = \sqrt{8}\,x.$$

Wir wollen unsere Resultate jetzt noch anwenden auf zwei Probleme, die in die allgemeine Transformationstheorie des siebenten Abschnittes gehören.

§ 132. Die Schlaeflische Modulargleichung für den 23sten Transformationsgrad.

Jede Klassengleichung tritt als Divisor in einer großen Zahl von Transformationsgleichungen auf und kann daher, wenn sie auf andere Weise bekannt ist, zur Berechnung von Transformationsgleichungen benutzt werden. Wir nehmen als Beispiel den 23sten Transformationsgrad.

Nach § 73 besteht, wenn

$$(1) \quad u = f(\omega), \quad v = f(23\,\omega), \quad f\left(\frac{c + \omega}{23}\right), \quad c \equiv 0 \pmod{48}$$

gesetzt ist, eine Gleichung zwischen

$$(2) \qquad A = \left(\frac{u}{v}\right)^{12} + \left(\frac{v}{u}\right)^{12}, \qquad B = uv + \frac{2}{uv},$$

und es ist schon in § 74, (14) gezeigt, daß diese Gleichung die Form hat:

$$(3) \qquad A = B^{11} + m_1 B^{10} + \cdots + m_{10} B + m_{11},$$

worin die Koeffizienten $m_1, m_2 \ldots, m_{11}$ rationale Zahlen sind. Statt nun diese rationalen Zahlenkoeffizienten wie dort aus den Entwickelungen von u und v nach Potenzen von q zu berechnen, suchen wir die Wurzeln der Gleichung (3) für $u = v$ aus der komplexen Multiplikation zu bestimmen.

Durch Multiplikation mit $u^{12}v^{12}$ geht die Gleichung (3) in eine Form über, welche u, v nicht im Nenner enthält, die wir für den Augenblick mit

(4) $$F(u, v) = 0$$

bezeichnen, so daß für ein unbestimmtes x und ω:

(5) $$F[f(\omega), x] = [x - f(23\,\omega)] \prod \left[x - f\left(\frac{c + \omega}{23}\right)\right].$$

Wir untersuchen nun, für welche Werte von ω die Funktion:

(6) $$F(u, u) = F[f(\omega), f(\omega)]$$
$$= [f(\omega) - f(23\,\omega)] \prod \left[f(\omega) - f\left(\frac{c + \omega}{23}\right)\right]$$

verschwindet. Es verschwindet zunächst offenbar der Faktor:

$$f(\omega) - f\left(\frac{\omega}{23}\right)$$

für

$$u = f(\sqrt{-23}) = f\left(\frac{\sqrt{-23}}{23}\right).$$

Verstehen wir ferner unter r eine der Zahlen ± 2 oder ± 4, und dementsprechend unter

$$m = 23 - r^2$$

entweder 19 oder 7, so verschwinden von den Faktoren von (6) für $\omega = \sqrt{-m}$ je zwei, nämlich:

$$f(\omega) - f\left(\frac{24\,r + \omega}{23}\right),$$

denn es ist

$$f\left(\frac{24\,r + \sqrt{-m}}{23}\right) = e^{\frac{r\pi i}{24}} f\left(\frac{r + \sqrt{-m}}{23}\right)$$
$$= e^{\frac{r\pi i}{24}} f\left(\frac{1}{r - \sqrt{-m}}\right) = f(\sqrt{-m}).$$

Wir fügen noch hinzu, daß

$$\frac{f(\omega) - f\left(\frac{24\,r + \omega}{23}\right)}{f(\omega) - f(\sqrt{-m})}$$

für $\omega = \sqrt{-m}$ einer endlichen Grenze zustrebt, wie man durch Differentiation nach ω erkennt (§ 54), und daraus folgt, daß $F(u, u)$ durch $[u - f(\sqrt{-m})]^2$ teilbar ist.

Wenn man $u = v$ setzt, so wird

$$A = 2, \quad B = u^2 + \frac{2}{u^2},$$

und wenn $u = f(\sqrt{-m})$, $m = 7, 19, 23$ gesetzt wird, so erhält man aus § 128, (6), (8), § 131, (1) durch Elimination von u die Gleichungen für B:

$$m = 7, \quad B - 3 = 0,$$
$$m = 19, \quad B^2 - 6B^2 + 10B - 6 = 0,$$
$$m = 23, \quad B^3 - 5B^2 + 4B - 1 = 0.$$

Die beiden letzten kubischen Gleichungen sind, da sie keine rationale Wurzel haben, irreducibel, und daraus ergibt sich ohne Rechnung die gesuchte Modulargleichung (3):

(7) $$A - 2 = (B-3)^2 (B^3 - 6B^2 + 10B - 6)^2 (B^3 - 5B^2 + 4B - 1).$$

In der Abhandlung: „Ein Beitrag zur Transformationstheorie der elliptischen Funktionen mit einer Anwendung auf Zahlentheorie“, Math. Annalen 43, 185, habe ich auf demselben Wege auch noch die Transformationsgleichung für den 47sten Transformationsgrad abgeleitet.

§ 133. Die Resolventen 7ten und 11ten Grades für den 7ten und 11ten Transformationsgrad.

Wir haben in § 82 gesehen, daß für den 7ten und 11ten Transformationsgrad Resolventen der Grade 7 und 11 existieren. Auch bei der Bildung dieser Gleichungen kann die Theorie der komplexen Multiplikation nützliche Dienste leisten.

Wir betrachten, wenn $n = 7$ oder $= 11$ ist, die Transformationsgleichung

$$F_n(u, v) = 0,$$

deren Wurzeln, wenn $u = f(\omega)$ gesetzt wird,

(1) $$v_\infty = f(n\omega), \quad v_c = f\left(\frac{\omega + c}{n}\right)$$

sind, wobei c als Index von v nach dem Modul n genommen werden kann, während es unter dem Zeichen f durch 48 teilbar vorausgesetzt werden muß.

Diese Gleichungen sind nach § 73:

(2) $$n = 7, \quad v^8 - u^7 v^7 + 7 u^4 v^4 - 8 u v + u^8 = 0,$$

(3) $$n = 11, \quad v^{12} - u^{11} v^{11} + 11 u^9 v^9 - 44 u^7 v^7 + 88 u^5 v^5 - 88 u^3 v^3 + 32 u v + u^{12} = 0.$$

Wir haben in § 73 den Einfluß der drei Vertauschungen

$$(4)\qquad \begin{aligned}(c') &= (\omega, \omega + 2),\\ (c'') &= \left(\omega, \frac{-1}{\omega}\right),\\ (c''') &= \left(\omega, \frac{\omega - 1}{\omega + 1}\right),\end{aligned}$$

durch die u übergeht in

$$e^{-\frac{\pi i}{12}} u, \quad u, \quad \frac{\sqrt{2}}{u},$$

auf die Wurzeln der Gleichungen (2) und (3) untersucht. Dieser Einfluß ergibt sich aus den Zusammensetzungen:

$$(5)\qquad \begin{pmatrix} n, & 0\\ c, & 1\end{pmatrix}\begin{pmatrix} 1, & 0\\ 2, & 1\end{pmatrix} = \begin{pmatrix} n, & 0\\ c', & 1\end{pmatrix},$$

$$(6)\qquad c' \equiv c + 2 \pmod{n};$$

$$(7)\qquad \begin{pmatrix} n, & 0\\ c, & 1\end{pmatrix}\begin{pmatrix} 0, & 1\\ -1, & 0\end{pmatrix} = \begin{pmatrix} -c'', & n\\ -\frac{c c'' + 1}{n}, & c\end{pmatrix}\begin{pmatrix} n, & 0\\ c'', & 1\end{pmatrix},$$

$$(8)\qquad c c'' \equiv -1 \pmod{n};$$

$$(9)\qquad \begin{pmatrix} n, & 0\\ c, & 1\end{pmatrix}\begin{pmatrix} 1, & 1\\ -1, & 1\end{pmatrix} = \begin{pmatrix} \alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix} 1, & 1\\ -1, & 1\end{pmatrix}\begin{pmatrix} n, & 0\\ c''', & 1\end{pmatrix},$$

$$(10)\qquad c''' \equiv \frac{c - 1}{c + 1} \pmod{n},$$

$$\alpha - \beta = 1 - c''', \quad \gamma + \delta = c + 1,$$
$$\alpha + \beta = n, \qquad n(\gamma - \delta) = (c - 1) - c'''(c + 1),$$

und nach § 34 und § 40, (12) geht also durch die Substitutionen (c'), (c''), (c'''), mit Rücksicht auf

$$2 \equiv 2 n^2 \pmod{48},$$

die Wurzel v_c über in:

$$(11)\qquad e^{-\frac{\pi i n}{12}} v_{c'}, \quad v_{c''}, \quad \left(\frac{2}{n}\right)\frac{\sqrt{2}}{v_{c'''}},$$

und dies gilt auch für $c = \infty$. Die Vertauschungen der Indices, die sich so ergeben, sind:

$$(12)\qquad n = 7, \quad \begin{aligned} c &= \infty, 0, 1, 2, 3, 4, 5, 6,\\ c' &= \infty, 2, 3, 4, 5, 6, 0, 1,\\ c'' &= 0, \infty, 6, 3, 2, 5, 4, 1,\\ c''' &= 1, 6, 0, 5, 4, 2, 3, \infty.\end{aligned}$$

$$(13)\qquad \begin{aligned} n = 11,\ c &= \infty,\ 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\\ c' &= \infty,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 0,\ 1,\\ c'' &= 0,\ \infty,\ 10,\ 5,\ 7,\ 8,\ 2,\ 9,\ 3,\ 4,\ 6,\ 1,\\ c''' &= 1,\ 10,\ 0,\ 4,\ 6,\ 5,\ 8,\ 7,\ 9,\ 2,\ 3,\ \infty. \end{aligned}$$

Als Wurzeln der Resolventen 7ten und 11ten Grades können wir nach § 82 je eine der beiden folgenden Funktionen betrachten:

$$(14)\qquad n = 7,$$

$$w_\nu = \frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+3})(v_{\nu+2} - v_{\nu+6})(v_{\nu+4} - v_{\nu+5})}{i\sqrt{7}\,u^4},$$

$$w'_\nu = \frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+5})(v_{\nu+2} - v_{\nu+3})(v_{\nu+4} - v_{\nu+6})}{-i\sqrt{7}\,u^4},$$

$$(15)\qquad n = 11,\quad w_\nu =$$

$$\frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+2})(v_{\nu+3} - v_{\nu+6})(v_{\nu+4} - v_{\nu+8})(v_{\nu+5} - v_{\nu+10})(v_{\nu+9} - v_{\nu+7})}{i\sqrt{11}\,u^6},$$

$$w'_\nu =$$

$$\frac{(v_\infty - v_\nu)(v_{\nu+1} - v_{\nu+6})(v_{\nu+3} - v_{\nu+7})(v_{\nu+4} - v_{\nu+2})(v_{\nu+5} - v_{\nu+8})(v_{\nu+9} - v_{\nu+10})}{-i\sqrt{11}\,u^6},$$

worin $\sqrt{7}$ und $\sqrt{11}$ positiv genommen sein sollen.

Es tritt nun zunächst der folgende bemerkenswerte Unterschied zwischen beiden Fällen hervor.

Durch die beiden Vertauschungen (c'), (c'') werden im Falle $n = 7$ die w_ν nur untereinander vertauscht, und zwar in folgender Weise:

$$\begin{array}{lccccccc} & w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6,\\ (c') & w_2, & w_3, & w_4, & w_5, & w_6, & w_0, & w_1,\\ (c'') & w_0, & w_2, & w_1, & w_6, & w_4, & w_5, & w_3, \end{array}$$

während [nach (13)] im Falle $n = 11$ durch die Vertauschung (c') die Größen w gleichzeitig ihr Vorzeichen ändern, so daß folgende Vertauschungen eintreten:

$$\begin{array}{lccccccccccc} & w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6, & w_7, & w_8, & w_9, & w_{10},\\ (c') & -w_2, & -w_3, & -w_4, & -w_5, & -w_6, & -w_7, & -w_8, & -w_9, & -w_{10}, & -w_0, & -w_1,\\ (c'') & w_0, & w_9, & w_6, & w_3, & w_5, & w_4, & w_2, & w_8, & w_7, & w_1, & w_{10}, \end{array}$$

und ebenso verhält es sich mit w'.

Daraus folgt nun (§ 54), daß die w_ν Wurzeln einer Gleichung 7ten oder 11ten Grades:

$$(16)\qquad w^n + A_1 w^{n-1} + A_2 w^{n-2} + \cdots + A_n = 0$$

sind, daß darin aber im Falle $n = 7$ sämtliche A_i rational von $f(\omega)^{24}$ abhängen, dagegen im Falle $n = 11$ die A_i mit geradem Index ebenfalls rational von $f(\omega)^{24}$ abhängen, während die mit ungeradem Index das Produkt von $f(\omega)^{12}$ mit einer rationalen Funktion von $f(\omega)^{24}$ sind. Die Zahlkoeffizienten enthalten außer rationalen Zahlen nur noch die Irrationalität $i\sqrt{7}$ bzw. $i\sqrt{11}$, und demnach wollen wir diese Gleichungen bezeichnen durch

$$(17) \qquad \begin{aligned} \Phi\left[w, f(\omega)^{24}, \; i\sqrt{7}\right] &= 0, \\ \Phi\left[w, f(\omega)^{12}, \; i\sqrt{11}\right] &= 0. \end{aligned}$$

Ändern wir gleichzeitig die Vorzeichen von i und w, so ergibt sich, wie wir in § 82 gesehen haben, eine Gleichung, deren Wurzeln die Größen w' sind.

Auch bei der Anwendung der Substitution (c''') zeigt sich für die beiden Fälle ein Unterschied.

Es ergibt sich nämlich aus (13), mit Rücksicht darauf, daß nach (2) das Produkt sämtlicher v_ν den Wert u^8 hat, daß im Falle $n = 7$ durch die Substitution (c''') die w_ν nur untereinander vertauscht werden, und zwar in folgender Weise:

$$\begin{pmatrix} w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6 \\ w_5, & w_3, & w_6, & w_2, & w_4, & w_0, & w_1 \end{pmatrix},$$

und daraus folgt, daß in diesem Falle die Koeffizienten A_ν alle ungeändert bleiben, durch die Vertauschung:

$$\left(f(\omega)^{24}, \; \frac{2^{12}}{f(\omega)^{24}}\right).$$

Überdies kommen im Nenner dieser Koeffizienten nur Potenzen von $f(\omega)^{24}$ vor (§ 73), und die Potenzen von $f(\omega)^{24}$ steigen bis zu derselben Höhe wie die von $f(\omega)^{-24}$.

Im Falle $n = 11$ gehen durch die Vertauschung (c''') die Größen w_ν in die Größen w'_ν über, und zwar in folgender Reihenfolge:

$$\begin{pmatrix} w_0, & w_1, & w_2, & w_3, & w_4, & w_5, & w_6, & w_7, & w_8, & w_9, & w_{10} \\ w'_8, & w'_2, & w'_7, & w'_0, & w'_9, & w'_5, & w'_6, & w'_4, & w'_3, & w'_{10}, & w'_1 \end{pmatrix}.$$

Nach (17) können wir diese Eigenschaft durch die in bezug auf w identische Gleichung ausdrücken:

$$-\Phi\left[-w, f(\omega)^{12}, -i\sqrt{11}\right] = \Phi\left(w, \frac{2^6}{f(\omega)^{12}}, i\sqrt{11}\right),$$

und daraus ergeben sich die folgenden Eigenschaften der Koeffizienten A_ν:

A_ν bleibt ungeändert durch die gleichzeitige Vertauschung:

$$\left(f(\omega)^{12}, \frac{64}{f(\omega)^{12}}\right), \quad (i\sqrt{11}, -i\sqrt{11}),$$

und enthält bei geradem ν nur die geraden, bei ungeradem ν nur die ungeraden Potenzen von $f(\omega)^{12}$.

Auch hier treten nur Potenzen von $f(\omega)$ im Nenner auf, und die Potenzen von $f(\omega)$ steigen bis zur selben Höhe wie die von $f(\omega)^{-1}$.

Um über die Grade der Funktionen A_ν ins Klare zu kommen, betrachten wir die Anfänge der Entwickelungen nach steigenden Potenzen von $q = e^{\pi i \omega}$.

Es beginnt die Entwickelung von $f(\omega)$ mit $q^{-\frac{1}{24}}$, die von v_∞ mit $q^{-\frac{n}{24}}$, von v_c mit $q^{-\frac{1}{24n}} e^{-\frac{2\pi i c}{48}\frac{1}{n}}$, worin aber in der letzten Exponentialgröße, wenn wir c auf seinen kleinsten Rest (mod n) reduzieren, auch $\frac{1}{48}$ nach dem Modul n zu nehmen, also für $n = 7, 11$:

$$\frac{1}{48} \equiv -1 \pmod{7},$$

$$\frac{1}{48} \equiv 3 \pmod{11}$$

zu setzen ist. Wenn wir also hiernach

$$\varrho = e^{\frac{2\pi i}{7}} \quad \text{oder} \quad = e^{-\frac{6\pi i}{11}}$$

setzen, so erhalten wir aus (14), (15) als Anfänge der Entwickelung

für $n = 7$:

$$i\sqrt{7}\, w_\nu = q^{-\frac{1}{7}} \varrho^{3\nu}(\varrho - \varrho^3)(\varrho^2 - \varrho^6)(\varrho^4 - \varrho^5) + \cdots,$$

für $n = 11$:

$$i\sqrt{11}\, w_\nu = q^{-\frac{5}{22}} \varrho^{5\nu}(\varrho - \varrho^2)(\varrho^3 - \varrho^6)(\varrho^4 - \varrho^8)(\varrho^5 - \varrho^{10})(\varrho^9 - \varrho^7) + \cdots$$

Es ist aber für $n = 7$:

$$(\varrho - \varrho^3)(\varrho^2 - \varrho^6)(\varrho^4 - \varrho^5) = -\varrho - \varrho^2 - \varrho^4 + \varrho^3 + \varrho^5 + \varrho^6,$$

und für $n = 11$:

$$(\varrho - \varrho^2)(\varrho^3 - \varrho^6)(\varrho^4 - \varrho^8)(\varrho^5 - \varrho^{10})(\varrho^9 - \varrho^7) = \\ -\varrho - \varrho^3 - \varrho^4 - \varrho^5 - \varrho^9 + \varrho^2 + \varrho^6 + \varrho^8 + \varrho^7 + \varrho^{10}.$$

Da 1, 2, 4 die quadratischen Reste von 7; 1, 3, 4, 5, 9 die quadratischen Reste von 11 sind, so können diese beiden Summen nach Bd. I, § 179 bestimmt werden, und ergeben in den beiden Fällen:

$$i\sqrt{7} \quad \text{und} \quad -i\sqrt{11},$$

so daß

$$(18) \qquad \begin{aligned} w_\nu &= \quad q^{-\frac{1}{7}}\varrho^{3\nu} + \cdots, \quad n = 7, \\ w_\nu &= -q^{-\frac{5}{22}}\varrho^{5\nu} + \cdots, \quad n = 11. \end{aligned}$$

Hierdurch läßt sich eine obere Grenze ableiten, bis zu der in A_ν die Potenzen von $f(\omega)$ höchstens ansteigen können, wenn man noch beachtet, daß die A_ν als ganze rationale (und symmetrische) Funktionen der w_ν darstellbar sind.

Für $n = 7$ ergibt sich so, da alle Exponenten von $f(\omega)$ durch 24 teilbar sein müssen, daß $A_1, A_2, A_3, A_4, A_5, A_6$ Konstanten sind, während A_7 nur die erste Potenz von $f(\omega)^{24}$, und zwar mit dem Koeffizienten -1 [nach (18)], enthält.

Für $n = 11$ muß, wenn $f(\omega)^{12\lambda}$ die höchste in A_ν vorkommende Potenz von $f(\omega)$ ist,

$$\lambda \overline{\gtrless} \frac{5\nu}{11}$$

sein, und überdies muß λ mit ν zugleich gerade oder ungerade sein. Daher sind A_2, A_4 konstant, A_6, A_8 enthalten die höchste Potenz $f(\omega)^{24}$, A_{10} enthält auch $f(\omega)^{48}$. Da die A mit ungeradem Index nur ungerade Potenzen von $f(\omega)^{12}$ enthalten, so ist $A_1 = 0$, A_3, A_5 enthalten $f(\omega)^{12}$, A_7, A_9 enthalten bis $f(\omega)^{36}$, in A_{11} steigt $f(\omega)$ bis zur 60sten Potenz an.

Für den Fall $n = 7$ wollen wir nun die Konstanten vollständig mit Hilfe der komplexen Multiplikation bestimmen, und zwar genügt dazu die Betrachtung der Werte der w_ν für $\omega = i$.

Für $\omega = i$ wird

$$u = f(i) = \sqrt[4]{2},$$

und wenn wir diesen Wert in die Gleichung (2) einführen, und

$$\sqrt[4]{2}\, v = x$$

setzen, so ergibt sich:

$$(19) \qquad x^8 - 4x^7 + 28x^4 - 32x + 16 = 0.$$

Die linke Seite dieser Gleichung ist das Quadrat des Ausdruckes:

$$(20) \qquad x^4 - 2x^3 - 2x^2 - 4x + 4,$$

so daß also die Werte von v für $\omega = i$ paarweise einander gleich werden. Aus § 119, (15), (17) folgt, wenn $\omega = i$, also $A = 1$, $C = 1$, $B = 0$, $m = 4$, $p = x = 7$, $y = 0$ gesetzt wird, daß für $cc' \equiv -1 \pmod 7$ $v_c = v_{c'}$ wird, so daß also:

(21) $$v_\infty = v_0, \quad v_1 = v_6, \quad v_2 = v_3, \quad v_4 = v_5.$$

Der Ausdruck (20) läßt sich in die beiden quadratischen Faktoren:

$$x^2 - (1 + \sqrt{7})\, x + 2, \quad x^2 - (1 - \sqrt{7})\, x + 2$$

zerlegen, so daß die acht Werte von x paarweise je einer der vier Größen

(22) $$\frac{1+\sqrt{7}}{2} \pm \frac{\sqrt[4]{7}}{\sqrt{2}}, \quad \frac{1-\sqrt{7}}{2} \pm i\frac{\sqrt[4]{7}}{\sqrt{2}}$$

gleich werden, und es handelt sich noch darum, diese vier Werte den einzelnen v_ν zuzuordnen. Dazu bemerken wir, daß v_∞, v_0 für $\omega = i$ reell sind, und daß ebenso v_1, v_6 reell sein müssen, weil sie gleichzeitig einander gleich und konjugiert imaginär sind.

Aus v_0 entsteht v_ν dadurch, daß man q mit einer gewissen Einheitswurzel multipliziert; da aber die Entwickelung von v_0 nach Potenzen von q nur positive Koeffizienten enthält [vgl. § 24, (11)], so folgt, daß v_0 größer sein muß als v_1, und mithin ist

(23) $$\begin{aligned}\sqrt[4]{2}\, v_\infty &= \sqrt[4]{2}\, v_0 = \frac{1+\sqrt{7}}{2} + \frac{\sqrt[4]{7}}{\sqrt{2}},\\ \sqrt[4]{2}\, v_1 &= \sqrt[4]{2}\, v_6 = \frac{1+\sqrt{7}}{2} - \frac{\sqrt[4]{7}}{\sqrt{2}}.\end{aligned}$$

Für die beiden anderen Wurzelpaare ergibt sich:

(24) $$\begin{aligned}\sqrt[4]{2}\, v_2 &= \sqrt{2}\, v_3 = \frac{1-\sqrt{7}}{2} + i\frac{\sqrt[4]{7}}{\sqrt{2}},\\ \sqrt[4]{2}\, v_4 &= \sqrt{2}\, v_5 = \frac{1-\sqrt{7}}{2} - i\frac{\sqrt[4]{7}}{\sqrt{2}}.\end{aligned}$$

Daß in diesen Ausdrücken das Vorzeichen von i richtig gewählt ist, schließt man auf folgende Weise:

Aus (23) ist zu ersehen, daß für $\omega = i$, also für $u = \sqrt{2}$, die Wurzel w_0 verschwindet, und daß also für diesen Wert A_7 verschwinden muß. Nach den oben nachgewiesenen Eigenschaften ist hierdurch A_7 vollständig bestimmt, nämlich:

(25) $$A_7 = -\left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

woraus folgt, daß für keinen anderen Wert von u^{24} als 64 zwei der Werte v_ν einander gleich werden. Es tritt diese Gleichheit also nur für $\omega = i$ und gewisse mit i äquivalente Werte von ω ein, und daher nicht für einen anderen rein imaginären Wert von ω.

Der Anfang der Entwickelung nach steigenden Potenzen von q ergibt nun:

$$(26)\qquad v_2 - v_5 = f\left(\frac{\omega - 2 \cdot 48}{7}\right) - f\left(\frac{\omega + 2 \cdot 48}{7}\right)$$
$$= 2 i q^{-\frac{1}{7 \cdot 24}} \sin \frac{4\pi}{7} + \cdots,$$

so daß für einen hinlänglich großen reellen Wert von $-i\omega$ die linke Seite von (26) positiv imaginär ist. Wenn nun $-i\omega$ auf reellem Wege von ∞ bis 1 geht, so geht, wie wir oben gesehen haben, $v_2 - v_5$ nicht durch Null. Es muß also auch für $\omega = i$ die Differenz $v_2 - v_5$ positiv imaginär sein, wie in (24) angenommen ist.

Wenn man also die Werte (23), (24) in (14) einsetzt, so ergibt sich für $\omega = i$:

$$w_0 = 0, \quad w_5 = 0$$
$$(27)\qquad w_1 = w_2 = w_3 = w_6 = \frac{7 + i\sqrt{7}}{2},$$
$$w_4 = -\frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}.$$

Danach kann für den Fall $n = 7$ die Resolvente vollständig gebildet werden. Sie lautet:

$$(28)\qquad w^2\left(w - \frac{7 + i\sqrt{7}}{2}\right)^4 \left(w + \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}\right)$$
$$= \left(u^{12} - \frac{64}{u^{12}}\right)^2,$$

und nimmt eine einfachere Gestalt an, wenn man

$$w + \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4} = z^2$$

setzt:

$$(29)\qquad z\left(z^2 - \frac{i\sqrt{7}\,(1 + i\sqrt{7})^2}{4}\right)\left(z^2 + i\sqrt{7}\right)^2 = u^{12} - \frac{64}{u^{12}}.$$

Für den Fall $n = 11$ ist die entsprechende Rechnung noch nicht durchgeführt. Verhältnismäßig einfach erhält man, wenn man mit Benutzung der Betrachtungsweise des § 119 die Werte von ω aufsucht, für die eine der Größen w_ν verschwindet:

$$\omega = i, \qquad \omega = \sqrt{-7}, \qquad \omega = \frac{1+\sqrt{-7}}{1-\sqrt{-7}},$$

$$u = \sqrt[4]{2}, \quad u = \sqrt{2}, \qquad u = 1,$$

und daraus

$$A_{11} = \left(u^{12} - \frac{2^6}{u^{12}}\right)^3 \left(u^{12} - \frac{2^{12}}{u^{12}}\right) \left(u^{12} - \frac{1}{u^{12}}\right).$$

Zwanzigster Abschnitt.

Die Multiplikatorgleichung in der komplexen Multiplikation.

§ 134. Die Klasseninvariante $\gamma_3(\omega)$.

Wir haben jetzt die Funktion

$$\gamma_3(\omega) = \sqrt{j(\omega) - 12^3}$$

auf deren Eigenschaft als Klasseninvariante zu prüfen.

Wir haben zunächst für ein variables ω die Multiplikatorgleichung 1ster Stufe (§ 72, 3), wonach, wenn

(1) $$n \equiv 3, \quad c \equiv 0 \pmod 4,$$

die ν Größe,

(2) $$M = (-1)^{\frac{a-1}{2}} \partial^3 \left(\frac{\eta\left(\frac{c+\partial\omega}{a}\right)}{\eta(\omega)} \right)^6 \gamma_3(\omega),$$

durch die linearen Transformationen nur miteinander permutiert werden. Setzen wir also

(3) $$u = j(\omega), \quad v = j\left(\frac{c+\partial\omega}{a}\right),$$

so besteht zwischen u, v die Invariantengleichung

(4) $$F(v, u) = 0,$$

und es ist

$$F(x, u) = \Pi(x - v),$$

wenn das Produktzeichen sich über die ν Wertsysteme von a, b, c erstreckt. Die Summe

(5) $$F(x, u) \sum \frac{M}{x - v} = \psi(x, u)$$

ist für ein unbestimmtes x durch lineare Transformation ungeändert und daher eine rationale Funktion von u. Da die Funktion aber für jeden endlichen Wert von $j(\omega)$ einen endlichen

Wert hat, so ist sie eine ganze Funktion von $j(\omega)$. Lassen wir in (5) x in v übergehen, so ergibt sich

$$M = \frac{\psi(v, u)}{F'(v)}, \tag{6}$$

worin $\psi(v, u)$ eine ganze rationale Funktion von u und v ist, mit rationalen Zahlenkoeffizienten.

Lassen wir nun in (6) ω in die Wurzel einer quadratischen Gleichung der negativen Diskriminante

$$D = B^2 - 4AC$$

übergehen:

$$A\omega^2 + B\omega + C = 0, \tag{7}$$

so können einer oder mehrere der Werte v gleich u werden. Ist dies nur für einen der ν Werte v der Fall, so wird $F'(v)$ für $v = u$ nicht verschwinden, und wir können nach (6) M rational durch diesen singulären Wert von u ausdrücken.

Die Gleichung $u = v$ führt aber die Bedingung mit sich:

$$\frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}.$$

Daraus folgt:

$$\begin{aligned} \partial\beta &= Ax, & \partial\alpha &= \frac{Bx - y}{2}, \\ c\beta - a\delta &= \frac{Bx + y}{2}, & c\alpha - a\gamma &= Cx, \end{aligned} \tag{8}$$

$$4n = y^2 - Dx^2, \tag{9}$$

worin x positiv angenommen werden kann.

Wir nehmen A ungerade und relativ prim zu D an. Ist $D \equiv 1 \pmod 4$, so setzen wir $n = -D$ und erhalten aus (9):

$$y^2 + n(x^2 - 4) = 0.$$

Der Wert $x = 1$ ist hiernach nur dann zulässig, wenn $-D$ das Dreifache einer Quadratzahl ist. Sehen wir zunächst von diesem Fall ab, so bleibt nur

$$x = 2, \qquad y = 0,$$

und aus (8) ergibt sich:

$$\begin{aligned} \partial &= 1, & \beta &= 2A, & \alpha &= B, \\ a &= n, & \gamma &\equiv 2C, & \delta &\equiv B \pmod 4, \end{aligned}$$
$$\alpha + \beta\omega = \sqrt{D},$$

und durch die beiden letzten Gleichungen (8) ist c nach dem Modul n bestimmt.

Nach § 38 (15) ist also

$$(10) \qquad M = (-1)^{A+C+\frac{B+1}{2}} \sqrt{D}^3 \gamma_3(\omega),$$

und es wird hier nur einer der Werte $v = u$, demnach ist M und folglich auch $\sqrt{D}\gamma_3(\omega)$ rational durch $j(\omega)$ ausdrückbar.

Um auch den Ausnahmefall zu erledigen, setzen wir

$$n = -D = 3m^2.$$

Dann wird (9):

$$y^2 + 3m^2(x^2 - 4) = 0,$$

und diese hat die drei Lösungen:

$$x = 2, \qquad y = 0,$$
$$x = 1, \qquad y = \mp 3m.$$

Die Gleichungen (8) ergeben für $x = 2$ wieder die Formel (10):

$$M_1 = (-1)^{A+C+\frac{B+1}{2}} \sqrt{D}^3 \gamma_3(\omega),$$

und die beiden anderen Fälle ergeben

$$\partial = 1, \qquad a = n,$$
$$\alpha = \frac{B \pm 3m}{2}, \quad \beta = A,$$
$$\gamma \equiv C, \qquad \alpha + \delta \equiv B \pmod 4,$$
$$\alpha + \beta\omega = \frac{\sqrt{D} \pm 3m}{2}.$$

Daraus erhält man nach § 38 (15) für M_2, M_3 die Werte

$$M_2 = (-1)^{\frac{B-1}{2}} \left(\frac{3m + \sqrt{D}}{2}\right)^3 \gamma_3(\omega),$$
$$M_3 = (-1)^{\frac{B-1}{2}} \left(\frac{-3m + \sqrt{D}}{2}\right)^3 \gamma_3(\omega).$$

Nun sind zwar nicht die Größen M_1, M_2, M_3 einzeln, wohl aber, wie wir gleich zeigen werden, ihre symmetrischen Funktionen, z. B. ihre Summe, durch $j(\omega)$ rational ausdrückbar, und daraus ergibt sich auch für diesen Fall, daß $\sqrt{D}\gamma_3(\omega)$ Klasseninvariante ist.

Von der Annahme, die wir gemacht haben, daß A relativ prim zu $2D$ sei, können wir uns nachträglich befreien, da $\gamma_3(\omega)$ durch alle linearen Transformatoren höchstens sein Zeichen ändert. Wir haben dann den Satz:

1. Ist $D \equiv 1 \pmod 4$, so ist $\sqrt{D}\gamma_3(\omega)$ Klasseninvariante der Diskriminante D.

Um den Satz vollständig zu begründen, müssen wir noch beweisen, daß die symmetrischen Funktionen der M_1, M_2, M_3 in dem zuletzt betrachteten Ausnahmefall rationale Funktionen von $j(\omega)$ sind. Dies erfordert, daß wir untersuchen, was aus (6) wird, wenn für einen singulären Wert u von v der Nenner $F'(v)$, und, da M endlich bleibt, auch der Zähler verschwindet. Wir lassen zunächst wieder ω variabel und bezeichnen die Wurzeln von (4) mit

(11) $$v_1, v_2, v_2, \ldots, v_\nu.$$

Es mögen nun für den betrachteten besonderen Wert von ω

(12) $$v_1, v_2, \ldots, v_\lambda$$

einander gleich werden, während die übrigen $v_{\lambda+1}, \ldots, v_\nu$ davon verschieden bleiben. Wir nehmen irgend eine symmetrische Funktion der Größe (12), z. B., für ein unbestimmtes t:

(13) $$\sigma = (t - v_1), (t - v_2), \ldots, (t - v_\lambda);$$

wenn wir in σ alle Permutationen der Größen (11) ausführen, so bestimmen wir r Werte

(14) $$\sigma_1, \sigma_2, \ldots, \sigma_r,$$

wenn
$$r = \frac{\nu!}{\lambda!\,(\nu - \lambda)!}$$
die Anzahl der Kombinationen von ν Größen zu je λ (ohne Wiederholung) bedeutet. Über t können wir so verfügen, daß auch für den singulären Wert ω nur eine der Größen (14) gleich dem ersten σ wird. Die σ sind die Wurzeln einer Gleichung
$$\Phi(x, u) = 0$$
vom Grade r, und für den singulären Wert $x = \sigma$ bleibt $\Phi'(\sigma)$ von Null verschieden.

Betrachten wir nun eine symmetrische Funktion S der (12) entsprechenden Größe
$$M_1, M_2, \ldots, M_\lambda,$$
so nimmt diese durch die ν Kombinationen der Zahlen $a, \mathfrak{d}, c$, die zu den Werten (11) führen, gleichfalls r Werte $S_1, S_2, \ldots, S_r$ an, und die Summe
$$\Phi(x, u) \sum \frac{S}{x - \sigma} = \Theta(x, u)$$
ist eine rationale ganze Funktion von x und u. Daraus folgt, indem man x in σ übergehen läßt:
$$S = \frac{\Theta(\sigma, u)}{\Phi'(u)}.$$

Für den singulären Wert werden nun alle die Größen (12) einander gleich und gleich u, also σ eine rationale Funktion von u, und damit ist der gesuchte Beweis geführt.

Als bemerkenswerte Beispiele wählen wir die Fälle des § 125:

$$\gamma_3\left(\frac{-1+\sqrt{-3}}{2}\right) = 24\sqrt{-3},$$

$$\gamma_3\left(\frac{-1+\sqrt{-7}}{2}\right) = 27\sqrt{-7},$$

$$\gamma_3\left(\frac{-1+\sqrt{-11}}{2}\right) = 7.\ 8\sqrt{-11},$$

$$\gamma_3\left(\frac{-1+\sqrt{-19}}{2}\right) = 8.\ 27\sqrt{-19},$$

$$\gamma_3\left(\frac{-1+\sqrt{-27}}{2}\right) = 8.\ 11.\ 23\sqrt{-3},$$

$$\gamma_3\left(\frac{-1+\sqrt{-43}}{2}\right) = 8.\ 7.\ 81\sqrt{-43},$$

$$\gamma_3\left(\frac{-1+\sqrt{-67}}{2}\right) = 7.\ 8.\ 9.\ 31\sqrt{-67},$$

$$\gamma_3\left(\frac{-1+\sqrt{-163}}{2}\right) = 8.\ 27.\ 7.\ 11.\ 19.\ 127\sqrt{-163}.$$

Auch hier ist die Zerlegbarkeit der rationalen Faktoren in verhältnismäßig kleine Primzahlen auffällig. Wir geben hier noch einige Beispiele, in denen nicht $\sqrt{D}$, sondern $\sqrt{-D}$ vorkommt.

Wir haben im § 128 gefunden:

$$f_1(\sqrt{-2})^4 = 2, \quad f(\sqrt{-3})^3 = 2, \quad f(\sqrt{-7})^2 = 2.$$

Darauf wenden wir die Formeln an (§ 129):

$$f_1^8 - f_2^8 = \frac{\sqrt{f^{24}-64}}{f^4},$$

$$f^8 + f_2^8 = \frac{\sqrt{f_1^{24}+64}}{f_1^4},$$

und finden

$$f(\sqrt{-2})^8 + f_2(\sqrt{-2})^8 = 4\sqrt{2},$$

$$f_1(\sqrt{-3})^8 - f_2(\sqrt{-3})^8 = \frac{4\sqrt{3}}{\sqrt[3]{2}},$$

$$f_1(\sqrt{-7})^8 - f_2(\sqrt{-7})^8 = 6\sqrt{7}.$$

Hieraus erhält man $\varkappa^2$ und $\varkappa'^2$ aus den Formeln [§ 54, (3)]

$$\varkappa^2 = \frac{f_2(\omega)^8}{f(\omega)^8}, \quad \varkappa'^2 = \frac{f_1(\omega)^8}{f(\omega)^8},$$

also

$$\omega = \sqrt{-2}: \quad \varkappa^2 = (\sqrt{2} - 1)^2,$$

$$\omega = \sqrt{-3}: \quad \varkappa^2 = \frac{2 - \sqrt{3}}{4} = \frac{(1 - \sqrt{3})^2}{8},$$

$$\omega = \sqrt{-7}: \quad \varkappa^2 = \frac{8 - 3\sqrt{7}}{16} = \frac{(3 - \sqrt{7})^2}{32}.$$

§ 135. Die Klasseninvariante $\varkappa^2$ und $\varkappa$.

Es ist in § 126 gezeigt, daß, wenn die Diskriminante D durch 4 teilbar ist, und die quadratische Gleichung, deren Wurzel ω ist, ungerade äußere Koeffizienten hat, $f(\omega)^{24}$ Klasseninvariante für die Diskriminante D ist.

Es ist aber nach § 54 und § 34

(1) $$\varkappa^2 \varkappa'^2 = \frac{16}{f(\omega)^{24}}, \quad \varkappa^2 = \frac{f_2(\omega)^8}{f(\omega)^8} = \frac{16}{f(\omega)^8 f_1(2\omega)^8}.$$

Genügt nun ω der Gleichung

(2) $$A\omega^2 + B\omega + C = 0$$

mit der Diskriminante

$$D = B^2 - 4AC,$$

so genügt $\omega' = 2\omega$ der Gleichung

$$A\omega'^2 + 2B\omega' + 4C = 0$$

mit der Diskriminante $4D$, und nach § 126, (13) ist daher $f_1(2\omega)^{24}$ Klasseninvariante für diese Diskriminante. Es ist also $\varkappa^2\varkappa'^2$ und $\varkappa^6$ rational ausdrückbar durch Klasseninvarianten der Diskriminante D und $4D$.

Die identische Gleichung

(3) $$\frac{\varkappa^2\varkappa'^2 + \varkappa^4\varkappa'^4 + 2\varkappa^6}{1 + \varkappa^6} = \varkappa^2$$

zeigt, daß dasselbe auch für den Modul $\varkappa^2$ gilt.

Da $\varkappa^2$ durch jede lineare Substitution in eine rationale (linear gebrochene) Funktion von $\varkappa^2$ übergeht, so kann jetzt auch die Voraussetzung, daß die Koeffizienten A, C ungerade sein sollen, fallen gelassen werden, und wir haben den Satz:

2. Ist die Diskriminante $D \equiv 0 \pmod 4$, so ist $\varkappa^2(\omega)$ Klasseninvariante der Diskriminante $4D$.

Im § 134 ist ferner nachgewiesen, daß für $D \equiv 1 \pmod 4$ $\sqrt{D}\,\gamma_3(\omega)$ Klasseninvariante ist. Es ist aber (§ 54)

$$(4) \qquad \gamma_3(\omega) = \frac{8(2 + \varkappa^2 \varkappa'^2)(\varkappa'^2 - \varkappa^2)}{\varkappa^2 \varkappa'^2}.$$

Genügt ω der Gleichung (2), und setzt man:

$$(5) \qquad \omega = \frac{\omega' - 1}{\omega' + 1},$$

so ergibt sich für ω' die Gleichung:

$$(6) \quad (A + B + C)\,\omega'^2 - 2(A - C)\,\omega' + (A - B + C) = 0.$$

Ist $D \equiv 5 \pmod 8$, so sind A, B, C ungerade, und ist $D \equiv 1 \pmod 8$, so können wir A und C gerade annehmen, und folglich ist in beiden Fällen (6) eine primitive Gleichung für ω' von der Diskriminante $4D$. Es ist daher nach § 126, 1. $f(\omega')^{24}$ eine Klasseninvariante für diese Diskriminante, und da nun nach § 34 (18)

$$f(\omega) f(\omega') = \sqrt{2}$$

ist, so gilt dasselbe für $f(\omega)^{24}$. Daraus folgt, daß $\varkappa^2 \varkappa'^2$ Klasseninvariante für $4D$ ist, und da man nach (4) $\varkappa^2$ rational durch γ_3 und $\varkappa^2 \varkappa'^2$ ausdrücken kann, so ergibt sich:

3. Ist die Diskriminante $D \equiv 1 \pmod 4$, so ist $\varkappa^2$ rational ausdrückbar durch eine Klasseninvariante der Diskriminante $4D$ und durch $\sqrt{D}$.

Ist $j(\omega)$ Klasseninvariante der Diskriminante D, so sind $j(2\omega)$, $j(\frac{1}{2}\omega)$ Klasseninvarianten für $4D$, und es ist:

$$(7) \qquad \begin{aligned} j(2\omega) &= \frac{(f_1(2\omega)^{24} + 16)^3}{f_1(2\omega)^{24}} = \frac{[256 + f_2(\omega)^{24}]^3}{f_2(\omega)^{48}} \\ &= \frac{16(16\varkappa'^2 + \varkappa^4)^3}{\varkappa^8 \varkappa'^2}, \\ j\left(\frac{\omega}{2}\right) &= \frac{\left[f_2\left(\frac{\omega}{2}\right)^{24} + 16\right]^3}{f_2\left(\frac{\omega}{2}\right)^{24}} = \frac{[256 + f_1(\omega)^{24}]^3}{f_1(\omega)^{48}} \\ &= \frac{16(16\varkappa^2 + \varkappa'^4)^3}{\varkappa^2 \varkappa'^8}. \end{aligned}$$

Hieraus ergibt sich, daß auch umgekehrt die Klasseninvarianten der Diskriminante $4D$ rational durch $\varkappa^2$ ausdrückbar sind.

Um auch $\varkappa(\omega)$ selbst als Klasseninvariante auffassen zu können, wendet man die Gausssche Transformation (§ 9, § 32) an. Danach ist:

$$\varkappa^2\left(\frac{\omega}{2}\right) = \frac{4\,\varkappa(\omega)}{[1+\varkappa(\omega)]^2},$$

woraus:

$$\varkappa(\omega) = \frac{\varkappa^2\left(\frac{\omega}{2}\right)[1+\varkappa^2(\omega)]}{4 - 2\,\varkappa^2\left(\frac{\omega}{2}\right)}.$$

Es ist also $\varkappa(\omega)$ rational ausgedrückt durch $\varkappa^2(\omega)$ und $\varkappa^2\left(\frac{\omega}{2}\right)$, und $\omega' = \frac{\omega}{2}$ genügt der Gleichung

(8) $$4\,A\,\omega'^2 + 2\,B\,\omega' + C = 0.$$

Ist C eine gerade Zahl, was wir annehmen können, wenn $D \equiv 0 \pmod 4$ oder $\equiv 1 \pmod 8$ ist, so kann in (8) der Faktor 2 weggehoben werden und die Diskriminante von (8) ist gleich D. Ist aber C ungerade, was bei $D \equiv 5 \pmod 8$ notwendig ist, so ist die Diskriminante von (8) gleich $4\,D$. Daraus folgt nach 2. und 3.:

4. a) Ist $D \equiv 0 \pmod 4$, so ist $\varkappa(\omega)$ rational ausdrückbar durch die Klasseninvarianten der Diskriminante $4\,D$.

b) Ist $D \equiv 1 \pmod 8$, so ist $\varkappa(\omega)$ ausdrückbar durch $\sqrt{D}$ und durch die Klasseninvarianten der Diskriminante $4\,D$.

c) Ist $D \equiv 5 \pmod 8$, so ist $\varkappa(\omega)$ rational ausdrückbar durch $\sqrt{D}$ und durch die Klasseninvarianten der Diskriminante $16\,D$.

§ 136. Quadratische Transformationsgrade.

Wenn der Transformationsgrad n eine ungerade Quadratzahl ist, so ist nach § 72, 5. für ein variables ω:

(1) $$M = (-1)^{\frac{a-1}{2}}\,\partial^3 \left(\frac{\eta\left(\frac{c+\partial\,\omega}{a}\right)}{\eta(\omega)}\right)^6,$$

wenn $a\partial = n$ und c durch 8 teilbar ist, eine ganze algebraische Funktion des Körpers $\mathfrak{R}(v, u)$, worin

$$(2) \qquad v = j\left(\frac{c + \partial\omega}{2}\right), \qquad u = j(\omega).$$

Es werde nun darin für ω eine Wurzel der primitiven quadratischen Gleichung

$$(3) \qquad A\omega^2 + B\omega + C = 0,$$

mit negativer Diskriminante

$$(4) \qquad D = B^2 - 4AC$$

gesetzt, und wir nehmen ein für allemal an, daß A positiv und relativ prim zu $2Dn$ sei, was keine Beschränkung ist. Soll nun $v = u$ werden, so ist dafür die notwendige und hinreichende Bedingung:

$$(5) \qquad \frac{c + \partial\omega}{a} = \frac{\gamma + \delta\omega}{\alpha + \beta\omega},$$

$$(6) \qquad \alpha\delta - \beta\gamma = 1.$$

Vergleicht man (5) mit (3), so folgt (§ 114), daß es zwei ganze positive Zahlen x, y geben muß, deren erste positiv angenommen werden kann und die den Bedingungen genügen:

$$(7) \qquad \begin{aligned} \partial\beta &= Ax, \qquad c\beta + \partial\alpha - a\delta = Bx, \\ c\alpha - a\gamma &= Cx, \quad -c\beta + \partial\alpha + a\delta = y, \\ 2\partial\alpha &= Bx + y, \\ 2(c\beta - a\delta) &= Bx - y, \end{aligned}$$

und daraus wegen (6):

$$(8) \qquad 4n = y^2 - Dx^2.$$

Ein Primteiler von ∂ müßte, da A relativ prim zu n angenommen ist, in x und in y aufgehen. Dann aber auch in

$$c\alpha - a\gamma \quad \text{und in} \quad c\beta - a\delta,$$

folglich in a, ∂, c. Da diese drei Zahlen aber ohne gemeinschaftlichen Teiler sind, so muß $\partial = 1$ sein, und aus (7) ergibt sich:

$$(9) \qquad \begin{aligned} \alpha &= \frac{Bx + y}{2}, \qquad \beta = Ax, \\ c\alpha - n\gamma &= Cx, \qquad c\beta - n\delta = \frac{Bx - y}{2}; \end{aligned}$$

daraus folgt, daß x und y keinen ungeraden gemeinschaftlichen Teiler haben, und daß, wenn x und y gerade sind, $\frac{1}{2}(Bx + y)$ ungerade sein muß. Da wir überdies x positiv annehmen können,

so kommen nur eigentliche Lösungen von (8) in Betracht (§ 114). Jede eigentliche Lösung führt aber nach (9) zu einem Wertsystem α, β, und durch die Kongruenzen

$$(10) \qquad c\alpha \equiv Cx, \qquad c\beta \equiv \frac{Bx - y}{2} \pmod{n}$$

zu einem bestimmten Wert von c (mod n), der auch noch durch 8 teilbar angenommen werden kann. Wenn umgekehrt x, y diesen Bedingungen genügen, so habe α und β keinen gemeinsamen Teiler, wie aus

$$\alpha \frac{Bx - y}{2} - \beta Cx = -n$$

hervorgeht. Denn danach müßte ein ungerader Teiler von α und β in n aufgehen, und müßte daher, da A relativ prim zu n angenommen war, in x und folglich in y aufgehen.

Es folgt aber noch, wenn wir von den beiden Ausnahmefällen $D = -3$, $D = -4$ absehen, die uns hier überhaupt nicht interessieren, weil für diese $j(\omega)$ rational ist, daß verschiedene Lösungen von (8) auch zu verschiedenen Werten c führen. Denn nehmen wir an, daß ein und derselbe Wert von c zu zwei verschiedenen Systemen (α, β, γ, δ) führen könnte, so würde aus (5) eine Relation der Form

$$\omega = \frac{\gamma + \delta\omega}{\alpha + \beta\omega}$$

folgen, und diese Substitution ist, wenn sie nicht identisch ist, nur für die beiden erwähnten Ausnahmefälle möglich.

Demnach ist die Anzahl der v-Werte in (2), die nach (3) gleich u werden, so groß wie die Anzahl der eigentlichen Lösungen der Gleichung (8).

Hat die Gleichung (8) nur eine solche Lösung, so ist der entsprechende Wert von M rational durch u ausdrückbar. Hat sie aber mehrere Lösungen, so sind die zugehörigen Werte von M die Wurzeln einer rationalen Gleichung:

$$(11) \qquad \Phi(M, u) = 0,$$

deren Grad in bezug auf M ebenso groß ist, wie die Anzahl dieser Lösungen (§ 134).

Es genügt ferner u der Klassengleichung

$$H_{-D}(u) = 0.$$

Wir können $\Phi(M, u)$ als ganze Funktion von u darstellen und können dann diese Funktion durch ihren größten gemeinschaftlichen Teiler mit $H_{-D}(u)$ ersetzen.

Wir können α und β positiv annehmen. Für β liegt dies in den bereits gemachten Voraussetzungen. Für α können wir es immer dadurch erreichen, daß wir B um ein Vielfaches von $2A$ vermehren, wodurch wir zu einer äquivalenten (parallelen) Form kommen. Dadurch kann $Bx + y$ positiv gemacht werden.

Bestimmen wir also den Quotienten

$$\frac{\eta\left(\dfrac{\gamma + \delta\omega}{\alpha + \beta\omega}\right)}{\eta(\omega)} = E\begin{pmatrix}\alpha, \beta\\ \gamma, \delta\end{pmatrix}$$

nach § 38, (15), so ergibt sich, da β gerade oder ungerade ist, je nachdem x gerade oder ungerade ist:

$$(12)\qquad \begin{aligned} x &\equiv 0 \pmod 2\colon\ M = \left(\frac{\beta}{\alpha}\right) i^{3\frac{\alpha-1}{2}} e^{\frac{\pi i}{4}\alpha(\gamma-\beta)} \sqrt{\alpha+\beta\omega}^{\,3},\\ x &\equiv 1 \pmod 2\colon\ M = \left(\frac{\alpha}{\beta}\right) i^{3\frac{1-\beta}{2}} e^{\frac{\pi i}{4}\beta(\alpha+\delta)} \sqrt{-i(\alpha+\beta\omega)}^{\,3}. \end{aligned}$$

Die Quadratwurzeln

$$(13)\qquad \begin{aligned} \sqrt{\alpha + \beta\omega} &= \sqrt{\frac{y + x\sqrt{D}}{2}},\\ \sqrt{-i(\alpha + \beta\omega)} &= \sqrt{-i\frac{y + x\sqrt{D}}{2}} \end{aligned}$$

haben positiven reellen Bestandteil. Diese Werte von M genügen also der Gleichung (11). Kommen unter ihnen gleiche vor, so kann der Grad der Gleichung (11) durch Absonderung mehrfacher Wurzeln auf rationalem Wege erniedrigt werden.

Da die Gleichung (11) zur Zerlegung der Klassengleichung nach den Vorzeichen von M angewandt werden soll, so ist es von Wichtigkeit, zu entscheiden, ob unter den zu demselben ω gehörigen Werten von M in (12) solche vorkommen, die sich nur durch das Vorzeichen unterscheiden.

Wir untersuchen, wann zwei verschiedene von den Werten (12), etwa M, M', dieselbe 8te Potenz haben. Ist

$$(14)\qquad M^8 = M'^8,$$

so muß, wenn ϱ eine zwölfte Einheitswurzel und x, y; x', y' zwei verschiedene Lösungen der Gleichung (8) sind:

$$(15)\qquad y' + x'\sqrt{D} = \varrho\,(y + x\sqrt{D}).$$

Daraus folgt, daß ϱ einer quadratischen Gleichung genügen muß, also daß

$$\varrho = \pm i \quad \text{oder} \quad \varrho = \frac{\pm 1 \pm \sqrt{-3}}{2} \tag{16}$$

sein muß, weil dies die einzigen nicht reellen zwölften Einheitswurzeln sind, die einer quadratischen Gleichung genügen, und $\varrho = \pm 1$ zu $x = x'$, $y = y'$ führen würde. Demnach muß $\sqrt{D}$ einem Körper angehören, der durch eine dieser Irrationalitäten ϱ bestimmt ist, d. h. es muß

$$D = -4m^2 \quad \text{oder} \quad D = -3m^2 \tag{17}$$

sein. Im ersten Fall folgt aus (15)

$$\begin{aligned} y' &= \pm 2mx, \\ 2mx' &= \mp y, \end{aligned} \tag{18}$$

also nach (8):

$$n = m^2(x^2 + x'^2),$$

und da n ungerade vorausgesetzt war, muß auch m ungerade sein; nach (18) sind y, y' und wegen (8) auch x, x' gerade, und aus (12) folgt, da γ und β gerade sind:

$$M^4 = (\alpha + \beta\omega)^6 = \left(\frac{y + ixm}{2}\right)^6,$$

und aus (18):

$$M'^4 = (\alpha' + \beta'\omega)^6 = \left(\frac{y' + ix'm}{2}\right)^6 = -\left(\frac{y + ixm}{2}\right)^6,$$

$$M'^4 = -M^4. \tag{19}$$

Es haben also M und M' nicht gleiche, sondern entgegengesetzte 4te Potenzen.

Im zweiten der Ausnahmefälle (17) folgt in gleicher Weise aus (15):

$$\begin{aligned} \pm 2y' &= y - 3mx, \\ \pm 2mx' &= y + mx. \end{aligned} \tag{20}$$

Darauf folgt, wenn man die oberen Zeichen nimmt,

$$m(x'y - y'x) = 2n, \tag{21}$$

und hieraus schließt man, daß m ungerade sein muß; denn wäre m gerade, so müßte y und y' gerade sein, und nach (21) wäre $2n$ durch 4, also n durch 2 teilbar. Dieser Fall ist also nicht weiter zu berücksichtigen, wenn wir ein gerades D voraussetzen.

Hiermit ist folgender Satz bewiesen:

1. Es sei $D \equiv 0 \pmod 4$ eine negative Diskriminante, x, y seien zwei Zahlen ohne gemeinsamen un-

geraden Teiler und so, daß, wenn x gerade ist, $y \equiv 2 \pmod 4$, ferner so, daß

$$n = \tfrac{1}{4}(y^2 - Dx^2)$$

eine ungerade Quadratzahl ist.

Es sei ferner M durch die Formel (12) bestimmt. Dann hat die Funktion $H_{-D}(u)$ einen Teiler

$$\Phi(M, u), \tag{22}$$

der mit keiner der Funktionen

$$\Phi(-M, u), \quad \Phi(iM, u), \quad \Phi(-i, Mu) \tag{23}$$

eine gemeinsame Wurzel hat.

§ 137. Zurückführung ungerader Diskriminanten auf gerade.

Nach einem von Kronecker ausgesprochenen Satz läßt sich die Klassengleichung unter Adjunktion von Quadratwurzeln in so viele Faktoren zerlegen, als es für die betreffende Klassengleichung Geschlechter der Formenklassen gibt, und zwar so, daß jedem dieser Faktoren nur die Klasseninvarianten genügen, für die die entsprechenden quadratischen Formen (A, B, C) zu einem und demselben Geschlecht gehören. Diese Zerlegung erhalten wir aus den im vorigen Paragraphen bewiesenen Satz 1.

Daß dieser Satz in der Form, in der wir ihn ausgesprochen haben, sich nur auf gerade Diskriminanten D bezieht, ist für den Beweis des Kroneckerschen Satzes keine Beschränkung.

Denn wenn $D \equiv 1 \pmod 8$ ist, dann ist nach § 123 der Klassenkörper $\mathfrak{K}(D)$ identisch mit dem Klassenkörper $\mathfrak{K}(4D)$. Ist aber $D \equiv 5 \pmod 8$, dann ist der Grad von $\mathfrak{K}(4D)$ dreimal so groß als der von $\mathfrak{K}(D)$, aber der letztere ist in dem ersteren enthalten, und die Anzahl der Geschlechter für $\mathfrak{K}(D)$ und $\mathfrak{K}(4D)$ ist die gleiche (§ 104).

Ist $u = j(\omega)$ eine Klasseninvariante für $D \equiv 1 \pmod 8$, so sind

$$v = j(\omega') = j(2\omega), \quad j\left(\frac{\omega}{2}\right), \quad j\left(\frac{\omega+1}{2}\right) \tag{1}$$

Klasseninvarianten von $4D$, und u ist eine rationale Funktion von v:

$$u = \varphi(v), \tag{2}$$

die ungeändert bleibt, welche der drei Größen (2) man auch für v setzen mag. Alle Charaktere der Formen, deren Wurzeln ω und ω' sind, haben denselben Wert.

Ersetzt man in (2) v durch eine andere Klasseninvariante derselben Diskriminante $4D$ und desselben Geschlechtes, so geht auch u in eine andere Klasseninvariante der Diskriminante D über, bleibt aber auch in demselben Geschlecht.

Läßt man also in (2) v die Klasseninvarianten eines Geschlechtes der Diskriminante $4D$ durchlaufen, so durchläuft u die Invarianten des entsprechenden Geschlechtes der Diskriminante D [indem es jeden dieser Werte dreimal, bei $D \equiv 1 \pmod 8$ nur einmal annimmt], und die symmetrischen Funktionen dieser u sind in dem gleichen Rationalitätsbereich enthalten wie die Größen v. Ist daher die Klassenfunktion $H_{-4D}(v)$ nach den Geschlechtern in Faktoren zerlegbar, so gilt das gleiche von $H_{-D}(u)$ [1]).

§ 138. Zerfällung der Klassengleichung nach den Geschlechtern.

Um den Satz 1., § 136, anzuwenden, setze man

$$D = B^2 - 4AC = -4m, \tag{1}$$

und zerlege m in zwei Faktoren

$$m = m'm'', \tag{2}$$

wobei vorausgesetzt ist, daß m'' ungerade und ohne quadratischen Teiler sei.

Nun machen wir in dem Satz 1., § 136, die Annahme:

$$\begin{aligned} x &= 4, \quad y = 2(4m' - m''), \\ n &= (4m' + m'')^2. \end{aligned} \tag{3}$$

$$\begin{aligned} \alpha &= 2B + 4m' - m'', \\ \alpha m'' &= 4AC - (B - m'')^2, \\ \beta &= 4A. \end{aligned} \tag{4}$$

$$\begin{aligned} \alpha + \beta\omega &= 2i\sqrt{m'm''} + 4m' - m'', \\ &= (2\sqrt{m'} + i\sqrt{m''})^2, \end{aligned} \tag{5}$$

[1]) Die Durchführung der entsprechenden Betrachtungen für ein ungerades D würde zwar auch möglich sein, würde aber zahlreiche Unterscheidungen und Weitläufigkeiten nötig machen. Hier ist ein Punkt, wo die Gausssche Bezeichnung und Unterscheidung von Formen erster und zweiter Art, deren ich mich noch in der ersten Auflage bedient habe, eine gewisse Vereinfachung des Ausdrucks mit sich bringen würde. Es hängt das mit der Ausnahmestellung zusammen, die die Zahl 2 in der ganzen Theorie der elliptischen Funktionen einnimmt, die in der Weierstrassschen Theorie etwas zurücktritt, aber doch nicht ganz verschwindet. Auf der anderen Seite ist diese Auszeichnung der Zahl 2 auch wieder die Quelle von großen Vereinfachungen, namentlich in den numerischen Resultaten.

worin die Quadratwurzeln positiv zu nehmen sind. Sodann ist, weil B gerade ist

$$\alpha m'' \equiv -1 \pmod 4, \quad \left(\frac{\beta}{\alpha}\right) = \left(\frac{A}{\alpha}\right),$$

und folglich nach dem Reziprozitätsgesetz und nach (4):

$$\left(\frac{\alpha m''}{A}\right) = \left(\frac{-1}{A}\right) = \left(\frac{-1}{A}\right)\left(\frac{A}{\alpha m''}\right),$$

also:

$$\left(\frac{A}{\alpha m''}\right) = 1.$$

(6)
$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{A}{m''}\right),$$

(7) $\beta \equiv 4, \quad \gamma \equiv 4\,C \pmod 8, \quad \alpha \equiv 1 \pmod 2$ [§ 136, (7)],

also:

$$e^{\frac{\pi i \alpha}{4}(\gamma-\beta)} = (-1)^{C-1},$$

ferner:

$$B + 2m' \equiv 2\,C \pmod 4,$$

also:

$$\frac{\alpha-1}{2} \equiv -\frac{m''+1}{2} + 2\,C \pmod 4,$$

$$i^{3\frac{\alpha-1}{2}} = (-1)^C i^{-3\frac{m''+1}{2}},$$

und demnach endlich nach § 136, (12), (13):

$$M = -\left(\frac{A}{m''}\right) i^{-3\frac{m''+1}{2}} (2\sqrt{m'} + i\sqrt{m''})^3,$$

wofür man auch setzen kann:

(8)
$$M = -\left(\frac{A}{m''}\right)\left(2\,i^{-\frac{m''+1}{2}}\sqrt{m'} + i^{-\frac{m''-1}{2}}\sqrt{m''}\right)^3.$$

Nach dem Satz 1. (§ 136) ist dann $H_{-D}(u)$ teilbar durch eine Funktion

$$\Phi(M, u),$$

die zu $\Phi(-M, u)$ relativ prim ist. Setzen wir

(9)
$$\mu = -\left(2\,i^{\frac{m''+1}{2}}\sqrt{m'} + i^{\frac{m''-1}{2}}\sqrt{m''}\right)^3,$$

so ist für jede Klasseninvariante von D eine der beiden Gleichungen

(10)
$$\Phi(\mu, u) = 0, \quad \Phi(-\mu, u) = 0$$

befriedigt, und zwar die erste oder die zweite, je nachdem

(11) $$\left(\frac{A}{m''}\right) = +1 \quad \text{oder} \quad \left(\frac{A}{m''}\right) = -1$$

ist.

2. Hieraus folgt, daß das Vorzeichen $\left(\frac{A}{m''}\right) = \pm 1$ nicht von der besonderen Form (A, B, C), sondern nur von der durch diese Form repräsentierten Klasse abhängt, also ein Charakter der Formenklasse ist.

Nun ist die Invariante einer zweiseitigen Klasse reell, und die Invarianten entgegengesetzter Klassen sind konjugiert imaginär. Für zwei entgegengesetzte Formen (A, B, C), $(A, -B, C)$ ist aber das Vorzeichen (11) das gleiche, und daraus folgt, daß $\Phi(\mu, u)$ entweder reelle oder konjugiert imaginäre Wurzeln, und folglich reelle Koeffizienten hat, und sich daher nicht ändert, wenn μ durch den konjugiert imaginären Wert μ' ersetzt wird. Nun sind die beiden Fälle $m'' \equiv 1$, $m'' \equiv 3 \pmod 4$ zu unterscheiden, weil es davon abhängt, welches Glied in (9) imaginär ist. Das eine Mal kommt i nur in der Verbindung $i\sqrt{m'}$, das andere Mal in $i\sqrt{m''}$ vor, und demnach ist:

(12) $$\Phi(\mu,u) = \tfrac{1}{2}[\Phi(\mu,u) + \Phi(\mu',u)] = \begin{cases} \Psi(\sqrt{m''},u) : m'' \equiv 1 \\ \Psi(\sqrt{m'},u) : m'' \equiv 3 \end{cases} \pmod 4.$$

Die Funktion Ψ, und folglich auch Φ, hat reelle Koeffizienten und enthält nur die eine der beiden Quadratwurzeln $\sqrt{m''}$, $\sqrt{m'}$. Die $\sqrt{m''}$ ist nach unserer Voraussetzung immer irrational, $\sqrt{m'}$ ist nur dann rational, wenn m' ein Quadrat ist. Da $H(u)$ rationale Koeffizienten hat, so muß es, wenn $m'' \equiv 1$ durch $\Psi(\sqrt{m''}, n)$ und $\Psi(-\sqrt{m''}, n)$, und wenn $m'' \equiv 3$, und m' kein Quadrat ist, durch $\Psi(\sqrt{m'}, n)$ und $\Psi(-\sqrt{m'}, n)$ teilbar sein.

Nun ändert M sein Vorzeichen durch die gleichzeitigen Vorzeichenänderungen:

(13) $$\begin{matrix} (i, -i), (\sqrt{m''}, -\sqrt{m''}) : m'' \equiv 1 \\ (i, -i), (\sqrt{m'}, -\sqrt{m'}) : m'' \equiv 3 \end{matrix} \pmod 4,$$

und folglich ist, wenn nicht $m'' \equiv 3$, und zugleich m' ein Quadrat ist, in beiden Fällen:

(14) $$H(u) = \Phi(M,u)\,\Phi(-M,u),$$

und diese Zerlegung ist nur dann nicht möglich, wenn $m'' \equiv 1 \pmod 4$ und zugleich m' ein Quadrat oder $m' = 1$ ist.

3. Jedes der beiden Vorzeichen (11) kommt in gleich vielen Klassen der Diskriminante $D = -4m'm''$ vor und die Klassenfunktion ist durch Adjunktion von

$$\left.\begin{array}{ll}\sqrt{m''}, & \text{wenn } m'' \equiv 1 \\ \sqrt{m''}, & \quad,, \quad m'' \equiv 3\end{array}\right\} \pmod 4$$

in zwei Faktoren vom Grade $\frac{1}{2}h$ zerlegbar, außer wenn $m'' \equiv 3$ und m' ein Quadrat ist.

In diesem Ausnahmefall ist, wenn wir $Q^2 = 4m'$ setzen, $-m'' = \varDelta$ der Stamm von

$$D = Q^2 \varDelta,$$

und es ist für jede durch eine Form der Diskriminante D darstellbare und zu D teilerfremde Zahl A:

$$(D, A) = \left(\frac{A}{m''}\right) = +1$$

und $H(u)$ ist mit $\varPhi(M, u)$ identisch.

Zerlegt man m in einer zweiten Art in zwei Faktoren

(15) $$m = m_1' m_1'',$$

wo m_1'' denselben Bedingungen genügt wie m'', so erhält man in gleicher Weise eine Zerlegung

(16) $$H(u) = \varPhi(M_1, u)\, \varPhi(-M_1, u),$$

und indem man den größten gemeinschaftlichen Teiler von $\varPhi(M, u)$ und $\varPhi(M_1, u)$ aufsucht, erhält man eine Zerlegung von $H(u)$ in vier Faktoren:

$$H(u) = \varPhi_1(u)\, \varPhi_2(u)\, \varPhi_3(u)\, \varPhi_4(u),$$

vorausgesetzt, daß in $\varPhi(M, u)$ eine Quadratwurzel einer Primzahl vorkommt, die in $\varPhi(M_1, u)$ nicht enthalten ist. So fährt man fort und zerlegt allmählich $H(u)$ in Faktoren, deren Anzahl eine Potenz von 2 ist.

Wir wollen die Anwendung auf die einzelnen Fälle etwas genauer betrachten.

1) Ist $m \equiv 3 \pmod 4$, so sind alle Charaktere in der Form

$$\left(\frac{A}{m''}\right)$$

enthalten, und die Formel (8) reicht hin, um alle Geschlechter voneinander zu trennen. Ist hier $m'' \equiv 3$, so ist $m' \equiv 1 \pmod 4$ und aus (12) folgt, daß in den Teilgleichungen nur die Quadratwurzeln aus solchen Zahlen vorkommen, die von der Form $4n + 1$

sind. Bezeichnen wir also mit $p, p', p'', \ldots$ die Primfaktoren von m von der Form $4n+1$, mit $q, q', q'', \ldots$ die Primfaktoren von m von der Form $4n+3$, so kommen in den Teilgleichungen die folgenden Quadratwurzeln vor:

$$\sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{qq'},\ \sqrt{qq''}, \ldots;$$

wenn also nur ein q in m enthalten ist, so kommt $\sqrt{q}$ in den Teilgleichungen nicht vor. Da in diesem Fall wenigstens ein q in m aufgehen muß, so ist die Anzahl der zur Zerlegung erforderlichen Quadratwurzeln gleich der Anzahl der in m aufgehenden Primzahlen, vermindert um 1, also gleich der Anzahl der diesem Fall entsprechenden unabhängigen Charaktere.

2) Ist

$$m \equiv 1 \pmod 4, \quad m \equiv 6,\ 2 \pmod 8, \quad m \equiv 4 \pmod{16},$$

so können nach § 105 beziehungsweise die Charaktere

$$\left(\frac{-1}{A}\right),\ \left(\frac{2}{A}\right),\ \left(\frac{-2}{A}\right),\ \left(\frac{-1}{A}\right)$$

durch die Charaktere von der Form

$$\left(\frac{A}{m''}\right)$$

ausgedrückt werden, und es reicht also auch in diesen Fällen die Formel (8) aus, um alle Geschlechter voneinander zu trennen.

Die Formeln (9), (12) lehren, daß in diesen Fällen zur vollständigen Trennung der Geschlechter folgende Adjunktionen nötig sind:

$$(17)\quad \begin{array}{ll} m \equiv 1 \pmod 4, & \sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{q},\ \sqrt{q'},\ \sqrt{q''}, \ldots \\ m \equiv 6 \pmod 8, & \sqrt{2},\ \sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{qq'},\ \sqrt{qq''}, \ldots \\ m \equiv 2 \pmod 8, & \sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{2q},\ \sqrt{2q'},\ \sqrt{2q''}, \ldots \\ m \equiv 4 \pmod{16}, & \sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{q},\ \sqrt{q'},\ \sqrt{q''}, \ldots \end{array}$$

Denn im Fall $m \equiv 1 \pmod 4$ ist die Anzahl der q jedenfalls gerade. Setzt man also $m = qr^2m''$, $m' = qr^2$ und versteht unter r^2 die größte in r^2m'' aufgehende Quadratzahl, so ist $m'' \equiv 3 \pmod 4$ und die Formel (12) gibt die Adjunktion von $\sqrt{q}$, also ist in diesem Fall zur vollkommenen Trennung der Geschlechter

$$\sqrt{p},\ \sqrt{p'},\ \sqrt{p''}, \ldots,\ \sqrt{q},\ \sqrt{q'},\ \sqrt{q''}, \ldots$$

zu adjungieren, und die Anzahl der Quadratwurzeln ist gleich der Anzahl der in m aufgehenden Primzahlen, wieder in Über-

einstimmung mit der Anzahl der unabhängigen Charaktere. Auf ähnliche Art ergeben sich die übrigen Fälle von (16).

In den noch übrigen Fällen, nämlich $m \equiv 12 \pmod{16}$ und $m \equiv 0 \pmod 8$, ist die vorstehende Zerlegung zwar auch noch anwendbar, in den so gewonnenen Teilgleichungen sind aber immer noch je zwei oder je vier Geschlechter vereinigt, entsprechend den Charakteren

$$\left(\frac{-1}{A}\right), \quad \left(\frac{2}{A}\right).$$

Wir leiten also noch eine zweite Transformationsformel wie (8) her, indem wir die Gleichung

$$4n = y^2 - Dx^2$$

(8), § 136, folgendermaßen befriedigen:

$$m = m'm'' \equiv 0 \pmod 4,$$

$$x = 2, \quad y = 2(m' - m''), \quad n = (m' + m'')^2,$$

worin wieder m'' ungerade und durch kein Quadrat teilbar angenommen ist, aber auch $= 1$ sein kann, und aus § 136, (9) erhält man

$$\alpha = B + m' - m'', \quad \beta = 2A, \quad \gamma \equiv -2C \pmod 8,$$

$$\alpha m'' = AC - (\tfrac{1}{2}B - m'')^2,$$

$$\sqrt{\alpha + \beta\omega} = \sqrt{m'} + i\sqrt{m''}.$$

Nehmen wir der Einfachheit halber $B \equiv 0 \pmod 8$, was nötigenfalls durch Übergang zu einer parallelen Form erreicht wird, so ergibt sich $m' \equiv C \pmod 8$, $\alpha \equiv C - m'' \pmod 8$ und folglich

$$i^{3\frac{\alpha-1}{2}} e^{\frac{\pi i}{4}\alpha(\gamma-\beta)} = (-1)^{\frac{1}{4}C} (-1)^{\frac{A+1}{2}} i^{3\frac{m''-1}{2}},$$

$$\left(\frac{\beta}{\alpha}\right) = \left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right)\left(\frac{2}{\alpha m''}\right)\left(\frac{A}{\alpha m''}\right).$$

$$\left(\frac{A}{\alpha m''}\right) = 1, \quad \left(\frac{2}{\alpha m''}\right) = (-1)^{\frac{1}{4}C},$$

und daraus ergibt sich nach § 136, (12), (13):

$$(18) \quad M = -\left(\frac{2}{m''}\right)\left(\frac{A}{m''}\right)\left(\frac{-1}{A}\right)\left(i^{\frac{m''-1}{2}}\sqrt{m'} + i^{\frac{m''+1}{2}}\sqrt{m''}\right)^3.$$

Diese Formel ergänzt die vorige für den Fall $m \equiv 12 \pmod{16}$, und zeigt, daß auch in diesem Falle die vollständige Zerfällung der Klassengleichung durch Adjunktion von

$$\sqrt{p}, \sqrt{p'}, \sqrt{p''}, \ldots, \sqrt{q}, \sqrt{q'}, \sqrt{q''}, \ldots$$

geschieht.

Ist nun m durch eine noch höhere als die zweite Potenz von 2 teilbar, so kann man, wenn der Exponent von 2 ungerade ist, nach § 105, (7) alle Charaktere auf solche von der Form

$$\left(\frac{A}{m''}\right), \quad \left(\frac{-1}{A}\right)\left(\frac{A}{m''}\right)$$

zurückführen. Man setze

$$m = 2r^2 m'',$$

indem man wieder unter r^2 die größte in $\frac{1}{2}m$ aufgehende Quadratzahl versteht und wende, je nachdem $m'' \equiv 1$ oder $\equiv 3 \pmod 4$ ist, die Formel (8) oder (18) an. Man erhält dann die vollständige Zerfällung der Klassengleichung unter Adjunktion der Quadratwurzeln aus sämtlichen in m aufgehenden Primzahlen, ausschließlich $\sqrt{2}$.

Ist aber der Exponent der höchsten in m aufgehenden Potenz von 2 eine gerade Zahl, so genügt auch (18) noch nicht zur vollständigen Zerlegung der Klassengleichung. Man kann zwar hier wieder durch die Formeln (8), (18) durch Adjunktion sämtlicher $\sqrt{p}$ und $\sqrt{q}$ die Funktion H zerfällen, die $\sqrt{2}$ bekommt man aber dadurch nicht hinein, und es bleiben also immer noch je zwei Geschlechter in einer solchen Teilgleichung enthalten. Um auch diese noch zu trennen, leiten wir unter der Voraussetzung, daß m durch 8 teilbar sei, noch eine dritte Formel her.

Wir setzen

$$m = m' m'',$$

$$x = 1, \quad y = \tfrac{1}{2}m' - 2m'', \quad n = (\tfrac{1}{4}m' + m'')^2.$$

$$\sqrt{-i(\alpha + \beta\omega)} = e^{-\frac{\pi i}{4}}\left(\tfrac{1}{2}\sqrt{m'} + i\sqrt{m''}\right),$$

worin wieder m'' ungerade und durch kein Quadrat teilbar ist. Hier folgt aus § 136:

$$(19) \quad M = (-1)^{\frac{m}{8}} e^{\frac{\pi i}{4}Am''}\left(\frac{A}{m''}\right)\left(i^{-\frac{m''+1}{2}}\tfrac{1}{2}\sqrt{m'} + i^{-\frac{m''-1}{2}}\sqrt{m''}\right)^3.$$

Nachdem die Zerlegung nach den Charakteren $\left(\frac{A}{m''}\right)$ durch die Formeln (8) und (18) erledigt ist, handelt es sich nur noch um die Zerlegung nach den Charakteren

$$\left(\frac{-1}{A}\right), \quad \left(\frac{2}{A}\right),$$

d. h. nach dem Verhalten von A gegen den Modul 8. Es genügt daher, in der Formel (19) $m'' = 1$ zu setzen, wodurch man folgende vier Werte von M erhält:

$$
(20) \quad
\begin{aligned}
M &= (-1)^{\frac{m}{8}} \frac{1+i}{\sqrt{2}} \left(1 - i\tfrac{1}{2}\sqrt{m}\right)^3, & A &\equiv 1 \pmod 8, \\
M &= (-1)^{\frac{m}{8}} \frac{-1+i}{\sqrt{2}} \left(1 - i\tfrac{1}{2}\sqrt{m}\right)^3 = M', & A &\equiv 3 \pmod 8, \\
M &= (-1)^{\frac{m}{8}} \frac{-1-i}{\sqrt{2}} \left(1 - i\tfrac{1}{2}\sqrt{m}\right)^3 = M'', & A &\equiv 5 \pmod 8, \\
M &= (-1)^{\frac{m}{8}} \frac{1-i}{\sqrt{2}} \left(1 - i\tfrac{1}{2}\sqrt{m}\right)^3 = M''', & A &\equiv 7 \pmod 8.
\end{aligned}
$$

Die vier Werte von M gehen aus dem ersten hervor durch die Vertauschungen:

$$
(21) \quad
\begin{array}{cccc}
M, & \sqrt{2}, & i, & \sqrt{m}, \\
M', & -\sqrt{2}, & -i, & -\sqrt{m}, \\
M'', & -\sqrt{2}, & i, & \sqrt{m}, \\
M''', & \sqrt{2}, & -i, & -\sqrt{m}.
\end{array}
$$

Ist nun $\Phi(M, u) = 0$ in demselben Sinne wie oben die zwischen u und M bestehende Gleichung, so sind die vier Funktionen

$$\Phi(M, u), \quad \Phi(-M, u), \quad \Phi(iM, u), \quad \Phi(-iM, u)$$

ohne gemeinsamen Teiler, und wenn $\Phi(M, u)$ in $H(u)$ enthalten ist, so sind auch die drei anderen Funktionen $\Phi(-M, u)$, $\Phi(iM, u)$, $\Phi(-iM, u)$ in $H(u)$ enthalten, da die Vorzeichen der Irrationalitäten (20) beliebig geändert werden können. Es ist daher

$$H(u) = \Phi(M, u)\,\Phi(-M, u)\,\Phi(iM, u)\,\Phi(-iM, u),$$

und es kommt also jeder der vier Fälle

$$A \equiv 1, \quad A \equiv 3, \quad A \equiv 5, \quad A \equiv 7 \pmod 8$$

in gleich vielen Formenklassen der Diskriminante $-4m$ vor.

Eine Ausnahme tritt nur dann ein, wenn m ein Quadrat oder das Doppelte eines Quadrates ist, weil im ersten Falle $\sqrt{m}$ rational und daher nur die Vertauschung (M, M'') gestattet ist, im zweiten Falle $\sqrt{2}$ und $\sqrt{m}$ gleichzeitig ihr Zeichen ändern, also nur die Vertauschung (M, M') zulässig ist.

Aber es genügen auch schon diese Vertauschungen, um die Teilgleichung durch Adjunktion von $\sqrt{2}$ weiter zu zerfällen.

Im ersten Falle kommen nach § 105 nur die beiden Kongruenzen

$$A \equiv 1, \quad A \equiv 5 \pmod 8,$$

im zweiten Falle nur die beiden Kongruenzen

$$A \equiv 1, \quad A \equiv 3 \pmod 8$$

vor, und zwar wieder in gleich viel Formenklassen. Die vollständige Zerlegung der Klassengleichung nach den Geschlechtern erfordert, wenn m durch 8 teilbar ist, immer die Adjunktion der Wurzeln aus sämtlichen in m aufgehenden Primzahlen, einschließlich 2.

Man bemerkt, daß in diesen Betrachtungen ein neuer Beweis der von Gauss und Dirichlet bewiesenen Sätze über die Existenz der Geschlechter enthalten ist, freilich nur für negative Diskriminanten.

§ 139. Beispiele.

Zur wirklichen Ausrechnung der Zerfällung der Klassengleichung sind die Formeln des vorigen Paragraphen nur in beschränktem Maße anwendbar wegen des zu hohen Grades der Transformationsgleichungen. Wir werden nachher in einem Falle eine wenigstens nahe verwandte Methode zur Anwendung bringen. Ist die Klassengleichung bekannt, so läßt sich meist leichter die Zerlegung direkt finden, indem man einen Ansatz von bekannter Form mit unbestimmten Koeffizienten macht; so findet man aus den Formeln § 130, (2), (29), (37) die folgenden Teilgleichungen, worin das positive Zeichen der Quadratwurzel dem Hauptgeschlecht entspricht:

$$m = 50, \qquad f_1(\sqrt{-50}) = \sqrt[4]{2}\,x,$$

$$x^3 - x^2 = \frac{1 + \sqrt{5}}{2}(x + 1),$$

$$m = 26, \qquad f_1(\sqrt{-26})^2 = \sqrt{2}\,x,$$

$$x^3 - x^2 = \frac{3 + \sqrt{13}}{2}(x + 1),$$

$$m = 41, \qquad z = \frac{f(\sqrt{-41})^2}{\sqrt{2}} + \frac{\sqrt{2}}{f(\sqrt{-41})^2},$$

$$z^2 - \frac{5 + \sqrt{41}}{2} z + \frac{7 + \sqrt{41}}{2} = 0.$$

Um aber eine Anwendung unserer allgemeinen Methode zu geben, nehmen wir $m \equiv 3 \pmod 8$ an und setzen $D = -m$. Wir befriedigen die Gleichung:

$$4n = y^2 + m x^2,$$

indem wir setzen

$$m = m' m'',$$

$$x = 1, \quad y = \frac{m' - m''}{2}, \quad 4n = \left(\frac{m' + m''}{2}\right)^2,$$

wobei y und folglich n ungerade ausfällt. Es wird ferner nach § 136, (13)

$$\alpha + \beta\omega = \left(\frac{\sqrt{m'} + i\sqrt{m''}}{2}\right)^2.$$

Setzen wir unter der Voraussetzung, daß n durch 3 nicht teilbar ist,

$$(1) \qquad M = \left(\frac{c}{e}\right) i^{\frac{a-1}{2}} \sqrt{\partial}\, \frac{\eta\left(\frac{c + \partial\omega}{a}\right)}{\eta(\omega)},$$

so läßt sich M mit Anwendung von § 38, (15) bestimmen und man findet, wenn m'' denjenigen der beiden Faktoren m', m'' bedeutet, der modulo 4 mit 1 kongruent ist:

$$(2) \quad M = -\left(\frac{A}{m''}\right)(-1)^{\frac{m'-m''-2}{8}} e^{-\frac{\pi i}{3} A (m'-m'')} \frac{\sqrt{m''} - i\sqrt{m'}}{2}.$$

Um hiervon eine Anwendung zu machen, setzen wir $n = 25$, also

$$20 = m' + m'',$$

und folglich

$$\begin{aligned} m'' &= 1, & m' &= 19, & m &= 19, \\ m'' &= 17, & m' &= 3, & m &= 51, \\ m'' &= 13, & m' &= 7, & m &= 91, \\ m'' &= 9, & m' &= 11, & m &= 99. \end{aligned}$$

Legen wir die Form

$$\left(1, \; \frac{m' - m''}{2}, \; n\right)$$

zugrunde, so ist $A = 1$ zu setzen, und (2) ergibt:

$$(3) \qquad \begin{aligned} m &= 19, & M &= -\frac{1 - i\sqrt{19}}{2}, \\ m &= 51, & M &= e^{-\frac{\pi i}{3}} \frac{\sqrt{17} - i\sqrt{3}}{2}, \\ m &= 91, & M &= \frac{\sqrt{13} - i\sqrt{7}}{2}, \\ m &= 99, & M &= e^{\frac{\pi i}{3}} \frac{3 - i\sqrt{11}}{2}. \end{aligned}$$

Nun genügt nach § 72, (27), (28) M einer Transformationsgleichung, die, wenn

$$\chi = M^5 + 5M^4 + 15M^3 + 25M^2 + 25M$$
$$= M^3\left[\left(M + \frac{5}{M}\right)^2 + 5\left(M + \frac{5}{M}\right) + 5\right]$$

gesetzt wird, die Gestalt erhält:

$$(4) \qquad j(\omega) = \gamma_2(\omega)^3 = \frac{(\chi^2 + 10\chi + 5)^3}{\chi}.$$

Für $m = 19$ erhält man hieraus den schon oben (§ 125) gefundenen Wert

$$\gamma_2\left(\frac{-3 + \sqrt{-19}}{2}\right) = -96,$$

und für die drei übrigen Werte von m erhält man

$$j\left(\frac{-7+\sqrt{-51}}{2}\right) = -2^{14}.27(6263 + 1519\sqrt{17}),$$
$$(5) \quad \gamma_2\left(\frac{-3+\sqrt{-91}}{2}\right) = -48(227 + 63\sqrt{13}),$$
$$j\left(\frac{-1+\sqrt{-99}}{2}\right) = -2^{12}(4\,591\,804\,316 + 799\,330\,532\sqrt{33}).$$

Hieraus kann man zu kubischen Gleichungen für

$$f(\sqrt{-51})^{24}, \quad f(\sqrt{-91})^8, \quad f(\sqrt{-99})^{24}$$

gelangen, indem man von den Formeln Gebrauch macht (§ 34, § 54):

$$f_2\left(\frac{-r + \sqrt{-m}}{2}\right) = \frac{\sqrt{2}\,e^{-\frac{r\pi i}{24}}}{f(\sqrt{-m})},$$
$$\gamma_2\left(\frac{-r + \sqrt{-m}}{2}\right)e^{-\frac{r\pi i}{3}} = \frac{f(\sqrt{-m})^{24} - 16^2}{f(\sqrt{-m})^{16}},$$

worin $r = 7, 3, 1$; $m = 51, 91, 99$ zu setzen ist. Setzt man also für $r = 3$:

$$f(\sqrt{-m}) = x,$$

so erhält man:

$$(6) \qquad x^{24} + \gamma_2(\omega)x^{16} - 16^2 = 0,$$

und für $r = 7, 1$:

$$f(\sqrt{-m})^3 = 2x,$$

für diese beiden Fälle:

$$(7) \qquad x^{24} - [3 - 2^{-8}j(\omega)]x^{16} + 3x^8 - 1 = 0,$$

wo für $\gamma_2(\omega)$ und $j(\omega)$ die Werte (5) einzusetzen sind. Diese Gleichungen lassen sich noch zerlegen, und man erhält für x selbst viel einfachere Gleichungen:

$$
\begin{aligned}
& f(\sqrt{-51})^3 = 2x, \quad x^3 - 4x^2 - x - 1 = \sqrt{17}\,x^2, \\
(8) \quad & f(\sqrt{-91}) = x, \quad x^3 - 2x^2 - x - 2 = \sqrt{13}\,x, \\
& f(\sqrt{-99})^3 = 2x, \quad x^3 - 13x^2 - 4x - 1 = \sqrt{33}\,(2x^2 + x).
\end{aligned}
$$

Die Darstellung der Klasseninvarianten $j(\omega)$ durch eine einzige Quadratwurzel ist immer dann möglich, wenn zwei Geschlechter und in jedem Geschlecht eine Klasse vorhanden ist. Diese Werte von m finden sich in der Gaussschen Tafel der Klassenzahlen (Werke, Bd. II, S. 450 ff.) unter der Bezeichnung II, 3, von denen die auszuwählen sind, die $\equiv 3 \pmod 8$ sind. Ihre Anzahl ist aller Wahrscheinlichkeit nach endlich, wie die erwähnte Tafel aufweist; es sind die Zahlen:

$$
\begin{aligned}
m = 35,\ 51,\ 75,\ 91,\ 99,\ 115,\ 123,\\
147,\ 187,\ 235,\ 267,\ 403,\ 427.
\end{aligned}
$$

Wenn die Formenklassen in eine beliebige Anzahl von Geschlechtern zerfallen, aber in jedem Geschlecht nur eine Klasse enthalten ist, dann lassen sich nach dem in § 138 bewiesenen Satze alle Klasseninvarianten durch Quadratwurzeln ausdrücken. Von Euler und Gauss ist durch Induktion geschlossen, daß es nur eine endliche Anzahl, nämlich 65, solcher Diskriminanten gibt [1]). In der Abhandlung „Zur komplexen Multiplikation elliptischer Funktionen" (Mathematische Annalen, Bd. 33) habe ich diese Zahlen alle berechnet. Sie sind auch in der Tafel der Klasseninvarianten, die diesem Buche beigefügt ist, enthalten.

[1]) Euler, Nouv. Mém. de Berlin 1776, S. 338. Gauss, Disq. art. 303. Euler ist auf diese Zahlen auf einem anderen Wege gelangt, nämlich von der Aufgabe, große Primzahlen zu ermitteln (Vgl. die Straßburger Dissertation von Peter Meyer: Beweis eines von Euler entdeckten Satzes, betreffend die Bestimmung von Primzahlen, Straßburg 1906). Diese Zahlen sind:

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Einundzwanzigster Abschnitt.

Die Normen der Klasseninvarianten $f(\omega)$.

§ 140. Konvergenz einer unendlichen Reihe.

Wir betrachten eine beliebige quadratische Form

(1) $$\psi(x, y) = Ax^2 + 2Bxy + Cy^2$$

mit negativer Diskriminante

(2) $$-m = B^2 - AC,$$

in der vorläufig die Koeffizienten A, B, C nicht notwendig als ganze Zahlen betrachtet werden sollen, nur sollen sie reell sein. Nehmen wir x, y als rechtwinkelige Koordinaten in einer Ebene an, so entsprechen den ganzzahligen Werten von x, y die Gitterpunkte. Die Gleichung

$$\psi(x, y) = t$$

stellt für ein konstantes t eine Ellipse dar, und die Anzahl $Z(t)$ der Werte von ψ, für ganzzahlige x, y, die kleiner als t sind, ist gleich der Anzahl der im Innern dieser Ellipse gelegenen Gitterpunkte. Nach Bd. II, § 194, (5) nähert sich der Grenzwert des Verhältnisses $Z(t):t$ für ein unendlich großes t, dem Flächeninhalt der Ellipse $\psi = 1$, nämlich dem Werte $\pi : \sqrt{m}$. Also haben wir

(3) $$\operatorname{Lim} \frac{Z(t)}{t} = \frac{\pi}{\sqrt{m}}.$$

Lassen wir also in der unendlichen Reihe

(4) $$S = \sum^{x, y} \frac{1}{\psi(x, y)^s}$$

die Zahlen x, y alle ganzzahligen Werte, ausgenommen die Kombination $x = 0$, $y = 0$, durchlaufen, so ist nach Bd. II, § 196, 4 S für $s > 1$ konvergent, und es ist

(5) $$\operatorname{Lim}_{s=1} (s - 1) S = \frac{\pi}{\sqrt{m}}.$$

Im folgenden soll durch direkte Umformung der Summe S nachgewiesen werden, daß

$$S - \frac{\pi}{(s-1)\sqrt{m}}$$

für $s = 1$ einen endlichen Grenzwert hat und dieser Grenzwert soll bestimmt werden.

§ 141. Die Kroneckersche Grenzformel.

Wir ordnen die Glieder der Reihe

$$S = \sum^{x,y} \frac{1}{\psi(x, y)^s}$$

zunächst in der Weise an, daß wir die dem verschwindenden y entsprechenden Glieder absondern und von den übrigen je zwei, welche entgegengesetzten Werten von x und y entsprechen, zusammenfassen.

So erhalten wir:

(1) $$S = M_s + N_s,$$

wenn zur Abkürzung

(2) $$M_s = 2 \sum_{1,\infty}^{y} \sum_{-\infty,\infty}^{x} \frac{1}{(Ax^2 + 2Bxy + Cy^2)^s},$$

(3) $$N_s = 2 \sum_{1,\infty}^{x} \frac{1}{(Ax^2)^s}$$

gesetzt ist. Der Wert N, den N_s für $s = 1$ erhält, läßt sich, da die Reihe für $s = 1$ unbedingt konvergent bleibt, direkt bestimmen und ergibt:

(4) $$N = \frac{2}{A} \sum_{1,\infty}^{x} \frac{1}{x^2} = \frac{\pi^2}{3A}.$$

Um das Verhalten von M_s für $s = 1$ zu ermitteln, zerlegen wir die Funktion $\psi(x, y) = Ax^2 + 2Bxy + Cy^2$ in zwei konjugiert imaginäre lineare Faktoren:

$$Ax^2 + 2Bxy + Cy^2 = A(x + \omega_1 y)(x - \omega_2 y),$$

wenn

(5) $$\omega_1 = \frac{B + i\sqrt{m}}{A}, \quad \omega_2 = \frac{-B + i\sqrt{m}}{A}$$

so erklärt werden, daß $\sqrt{m}$ positiv ist.

Hierdurch wird

(6) $$M = \frac{2}{A^s} \sum_{1,\infty}^{y} \sum_{-\infty,\infty}^{x} \frac{1}{(x + \omega_1 y)^s (x - \omega_2 y)^s}.$$

Nun ist nach einem bekannten Satz aus der Theorie der Γ-Funktionen, wenn k eine beliebige Größe mit positiv imaginärem Bestandteil bedeutet:

$$\frac{1}{(-ik)^s} = \frac{(2\pi)^s}{\Gamma(s)} \int_0^\infty e^{2\pi i k \xi}\, \xi^{s-1}\, d\xi,$$

worin die Potenz $(-ik)^s$ dadurch eindeutig erklärt ist, daß, wenn $-ik = \varrho e^{i\Theta}$ gesetzt, ϱ positiv und der Winkel Θ zwischen $-\frac{\pi}{2}$ und $+\frac{\pi}{2}$ angenommen wird, $(-ik)^s = \varrho^s e^{i\Theta s}$ zu setzen ist.

Ersetzt man hierin ik durch die konjugiert imaginäre Größe $-ik'$, indem man zugleich einen neuen Integrationsbuchstaben η wählt, und multipliziert beide Gleichungen, so folgt:

$$(7) \qquad \frac{1}{(kk')^s} = \frac{(2\pi)^{2s}}{\Gamma(s)\Gamma(s)} \int_0^\infty \int_0^\infty e^{2\pi i (k\xi - k'\eta)} (\xi\eta)^{s-1}\, d\xi\, d\eta.$$

Hierin setzen wir für k, k' die beiden konjugierten Faktoren $x + \omega_1 y$, $x - \omega_2 y$ von ψ und führen den Integralausdruck (7) in (6) ein.

Dadurch erhalten wir:

$$(8) \quad M_s = \frac{(2\pi)^{2s}}{A_s \Gamma(s)\Gamma(s)} \sum^{x,y} 2 \int_0^\infty \int_0^\infty e^{2\pi i [x(\xi - \eta) + y(\omega_1 \xi + \omega_2 \eta)]} (\xi\eta)^{s-1}\, d\xi\, d\eta.$$

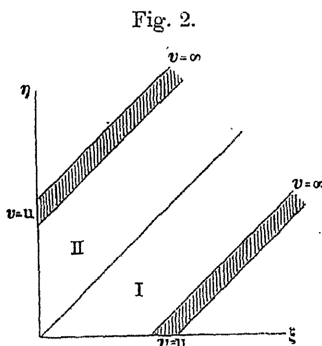
Wir fassen nun das Produkt der beiden Integrale auf der rechten Seite dieses Ausdruckes, das wir zur Abkürzung durch

$$(9) \qquad W = 2 \int_0^\infty \int_0^\infty e^{2\pi i [x(\xi - \eta) + y(\omega_1 \xi + \omega_2 \eta)]} (\xi\eta)^{s-1}\, d\xi\, d\eta$$

bezeichnen, als Doppelintegral auf, das sich, wenn ξ, η als rechtwinkelige Koordinaten in der Ebene gedeutet werden, über den positiven Quadranten des Koordinatensystems erstreckt.

Um das Doppelintegral umzuformen, teilen wir den Integrationsbereich durch eine den Winkel halbierende Gerade in die beiden Teile I, II (s. die Fig. 2), und substituieren im ersten Teil

Fig. 2.



$$\xi - \eta = u, \qquad \xi + \eta = v,$$

im zweiten Teil:

$$\xi - \eta = -u, \quad \xi + \eta. = v.$$

Wenn man dann, wie die Figur andeutet, zuerst bei konstantem u in bezug auf v integriert, so erhält man:

$$W = \int_0^\infty e^{2\pi i x u}\, d u \int_u^\infty e^{\pi i y\,[u(\omega_1 - \omega_2) + v(\omega_1 + \omega_2)]} \left(\frac{v^2 - u^2}{4}\right)^{s-1} d v,$$

$$+ \int_0^\infty e^{-2\pi i x u}\, d u \int_u^\infty e^{\pi i y\,[-u(\omega_1 - \omega_2) + v(\omega_1 + \omega_2)]} \left(\frac{v^2 - u^2}{4}\right)^{s-1} d v,$$

oder, wenn man zur Abkürzung

$$(10) \qquad \varphi_\pm(u) = \int_u^\infty e^{\pi i y\,[v(\omega_1 + \omega_2) \pm u(\omega_1 - \omega_2)]} \left(\frac{v^2 - u^2}{4}\right)^{s-1} d v$$

setzt,

$$(11) \qquad W = \int_0^\infty e^{2\pi i x u}\, \varphi_+(u)\, d u + \int_0^\infty e^{-2\pi i x u}\, \varphi_-(u)\, d u.$$

Diese nach u genommenen Integrale zerlegen wir in lauter solche Bestandteile, deren Grenzen die Reihe der ganzen Zahlen sind, wir setzen also, da x eine ganze Zahl ist:

$$(12) \qquad \int_0^\infty e^{\pm 2\pi i x u}\, \varphi_\pm(u)\, d u = \sum_{0,\infty}^{\nu} \int_\nu^{\nu+1} e^{\pm 2\pi i x u}\, \varphi_\pm(u)\, d u,$$

$$= \sum_{0,\infty}^{\nu} \int_0^1 e^{\pm 2\pi i x u}\, \varphi_\pm(u + \nu)\, d u,$$

$$= \int_0^1 e^{\pm 2\pi i x u} f(u)\, d u,$$

wenn wiederum

$$(13) \qquad f(u) = \sum_{0,\infty}^{\nu} \varphi_\pm(u + \nu)$$

gesetzt ist.

Wenn wir nun zunächst die Summation in bezug auf x ausführen, so können wir von der Grundformel aus der Theorie der Fourierschen Reihen Gebrauch machen:

$$(14) \qquad \sum_{-\infty,\infty}^{x} \int_0^1 e^{\pm 2\pi i x u} f(u)\, d u = \tfrac{1}{2}[f(0) + f(1)]$$

$$= \tfrac{1}{2}\varphi_\pm(0) + \sum_{1,\infty}^{\nu} \varphi_\pm(\nu),$$

und erhalten also, da nach (10)

$$(15)\qquad \varphi_+(0) = \varphi_-(0) = \varphi(0) = \int_0^\infty e^{\pi i y v(\omega_1+\omega_2)} \left(\frac{v}{2}\right)^{2s-2} dv$$

ist, aus (11), (12) und (14):

$$(16)\qquad \sum_{-\infty,\infty}^{x} W = \varphi(0) + \sum_{1,\infty}^{\nu} [\varphi_+(\nu) + \varphi_-(\nu)].$$

Führen wir dies in (8) ein, so zerfällt M_s in zwei Teile:

$$(17)\qquad M_s = P_s + Q_s,$$

wenn

$$(18)\qquad P_s = \frac{(2\pi)^{2s}}{A^s \Gamma(s)\Gamma(s)} \sum_{1,\infty}^{y} \varphi(0),$$

$$(19)\qquad Q_s = \frac{(2\pi)^{2s}}{A^s \Gamma(s)\Gamma(s)} \sum_{1,\infty}^{y} \sum_{1,\infty}^{\nu} [\varphi_+(\nu) + \varphi_-(\nu)]$$

gesetzt wird.

Nach (15) ist, wenn wir für v eine neue Integrationsvariable t durch die Gleichung

$$\pi i v(\omega_1 + \omega_2) = -\frac{2\pi v\sqrt{m}}{A} = -t$$

einführen, und die Summation nach y ausführen:

$$\sum_{1,\infty}^{y} \varphi(0) = \frac{2A^{2s-1}}{(4\pi\sqrt{m})^{2s-1}} \int_0^\infty \frac{t^{2s-2}\,dt}{e^t - 1},$$

also:

$$(20)\qquad P_s = \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\Gamma(s)^2}\, 2\int_0^\infty \frac{t^{2s-2}\,dt}{e^t-1}.$$

Hieraus läßt sich der Grenzwert P leicht bestimmen. Es ist nämlich das Integral

$$(21)\qquad \int_0^\infty t^{2s-2} e^{-t}\left(\frac{1}{1-e^{-t}} - \frac{1}{t}\right) dt,$$

da der in der Klammer stehende Ausdruck für $t = 0$ und $t = \infty$ einen endlichen Wert behält, bis $s = 1$ stetig, und hat daher den Grenzwert:

$$\int_0^\infty e^{-t}\left(\frac{1}{1-e^{-t}} - \frac{1}{t}\right) dt = -\Gamma'(1) = 0{,}5772\ldots$$

Zerlegt man also das Integral (21) in seine beiden Bestandteile und setzt

$$\int_0^\infty t^{2s-3} e^{-t} dt = \Gamma(2s-2) = \frac{\Gamma(2s-1)}{2(s-1)},$$

so folgt:

$$\operatorname*{Lim}_{s=1}\left(\int_0^\infty \frac{t^{2s-2}\,dt}{e^t-1} - \frac{\Gamma(2s-1)}{2(s-1)}\right) = -\Gamma'(1),$$

und wenn man also die Entwickelung nach Potenzen von $s-1$:

$$\Gamma(2s-1) = 1 + 2\Gamma'(1)(s-1) + \cdots$$

einsetzt,

$$(22) \qquad \operatorname*{Lim}_{s=1}\left\{2\int_0^\infty \frac{t^{2s-2}\,dt}{e^t-1} - \frac{1}{s-1}\right\} = 0.$$

Man erhält ferner durch Entwickelung nach Potenzen von $s-1$:

$$(23) \qquad \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\Gamma(s)^2}$$

$$= \frac{\pi}{\sqrt{m}}\left[1 + (s-1)\left(\log\frac{A}{4m} - 2\Gamma'(1)\right) + \cdots\right]$$

so daß nach (20):

$$(24) \qquad P_s = \frac{(2\pi)^{2s} A^{s-1}}{(4\pi\sqrt{m})^{2s-1}\Gamma(s)^2}\left(2\int_0^\infty \frac{t^{2s-2}\,dt}{e_t-1} - \frac{1}{s-1}\right)$$

$$+ \frac{\pi}{\sqrt{m}(s-1)} + \frac{\pi}{\sqrt{m}}\left(\log\frac{A}{4m} - 2\Gamma'(1)\right) + \cdots,$$

worin die noch folgenden Glieder mit $s-1$ verschwinden. Daraus folgt:

$$(25) \qquad \operatorname{Lim}\left(P_s - \frac{\pi}{\sqrt{m}(s-1)}\right) = \frac{\pi}{\sqrt{m}}\left(\log\frac{A}{4m} - 2\Gamma'(1)\right).$$

Es bleibt noch der Bestandteil Q_s zu untersuchen übrig, der für $s = 1$ einen endlichen Grenzwert Q erhält; diesen können wir ohne weiteres durch Einsetzen des Wertes $s = 1$ bestimmen.

Es läßt sich nämlich in (10), solange u und y größer als Null sind, nach Einsetzen des Wertes $s = 1$ die Integration

ausführen und ergibt mit Rücksicht auf den Wert $2i\sqrt{m}$ von $A(\omega_1 + \omega_2)$:

$$\varphi_{\pm}(\nu) = \frac{A}{2\pi\sqrt{m y}} e^{2\pi i y \nu \omega},$$

worin $\omega = \omega_1$ oder $= \omega_2$ zu setzen ist, je nachdem das obere oder untere Zeichen in $\varphi_{\pm}(\nu)$ genommen wird. Durch Ausführung der Summation nach y folgt hieraus:

$$\sum_{1,\infty}^{\nu} \sum_{1,\infty}^{y} \varphi_{\pm}(\nu) = -\frac{A}{2\pi\sqrt{m}} \sum_{1,\infty}^{\nu} \log(1 - e^{2\pi i \nu \omega}),$$

und die Summe nach ν läßt sich auf die Funktion $\eta(\omega)$ zurückführen, da nach § 24, (8):

$$\eta(\omega) = e^{\frac{\pi i \omega}{12}} \prod_{1,\infty}^{\nu} (1 - e^{2\pi i \nu \omega})$$

ist. Danach wird, immer für $s = 1$,

$$\sum_{1,\infty}^{\nu} \sum_{1,\infty}^{y} \varphi_{\pm}(\nu) = -\frac{A}{2\pi\sqrt{m}} \left(\log \eta(\omega) - \frac{\pi i \omega}{12}\right).$$

Führen wir dies Resultat in (19) ein, nachdem wir dort $s = 1$ gesetzt haben, so ergibt sich der Grenzwert von Q_s:

(26) $$Q = -\frac{2\pi}{\sqrt{m}} \log \eta(\omega_1)\,\eta(\omega_2) - \frac{\pi^2}{3A}.$$

Hiernach erhalten wir aus (4), (25), (26) die folgende Grenzformel, deren Ableitung das Ziel dieser Betrachtung war:

(27) $$\lim_{s=1} \sum^{x,y} \frac{1}{(Ax^2 + 2Bxy + Cy^2)^s} - \frac{\pi}{(s-1)\sqrt{m}}$$
$$= -\frac{2\pi\Gamma'(1)}{\sqrt{m}} + \frac{\pi}{\sqrt{m}} \log \frac{A}{4m} - \frac{2\pi}{\sqrt{m}} \log \eta(\omega_1)\,\eta(\omega_2).$$

Aus (27) ergibt sich in Übereinstimmung mit § 140, (5):

$$\lim\,(s-1) \sum^{x,y} \frac{1}{\psi^s} = \frac{\pi}{\sqrt{m}},$$

also nur abhängig von m, nicht von der besonderen Form ψ. Verstehen wir also jetzt unter A, $2B$, C ganze Zahlen und lassen ψ ein vollständiges Repräsentantensystem der zur Diskriminante $-4m$ gehörigen Formenklassen durchlaufen, so folgt

(28) $$\lim_{s=1}\,(s-1) \sum^{\psi} \sum^{x,y} \frac{1}{\psi^s} = \frac{\pi h}{\sqrt{m}},$$

wenn h die zur Diskriminante $-4m$ gehörige Klassenzahl ist.

Aus (27) leitet man eine einfachere Formel her für die Funktion

$$f(\omega) = e^{-\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)} = e^{\frac{\pi i}{24}} \frac{\eta\left(\frac{\omega-1}{2}\right)}{\eta(\omega)}.$$

Ersetzt man nämlich

$$\begin{array}{lll} A & \text{durch} & 2A, \\ B & \text{„} & A + B, \\ C & \text{„} & \frac{1}{2}(A + 2B + C), \end{array}$$

so bleibt $m = AC - B^2$ ungeändert und ω_1, ω_2 gehen über in

$$\omega_1' = \frac{\omega_1 + 1}{2}, \quad \omega_2' = \frac{\omega_2 - 1}{2}.$$

Setzt man also

$$(29) \qquad \begin{aligned} \psi &= (A,\ 2B,\ C), \\ \psi' &= [2A,\ 2(A+B),\ \tfrac{1}{2}(A + 2B + C)], \end{aligned}$$

so ergibt sich aus (27)

$$(30) \qquad \operatorname*{Lim}_{s=1} \left(\sum^{x,y} \frac{1}{\psi^s} - \sum^{x,y} \frac{1}{\psi'^s} \right) = \frac{2\pi}{\sqrt{m}} \log \frac{f(\omega_1) f(\omega_2)}{\sqrt{2}}.$$

Wir nehmen jetzt nicht nur A, $2B$, C, sondern auch A, B, C als ganze Zahlen ohne gemeinschaftlichen Teiler und A ungerade an. Dann ist ψ eine primitive Form der Diskriminante $-4m$, und wir betrachten zunächst die beiden Fälle

$$m \equiv 1, \qquad m \equiv 2 \pmod 4.$$

Nehmen wir, was keine weitere Beschränkung ist, $B \equiv m + 1 \pmod 2$ an, d. h. B gerade oder ungerade, je nachdem m ungerade oder gerade ist, so ergibt sich aus

$$m = AC - B^2:$$

$$\begin{array}{lll} A - C \equiv 0 & (\text{mod } 4) & m \text{ ungerade}, \\ A + C \equiv 0 & \text{„} & m \text{ gerade}, \end{array}$$

und die Form ψ' ist primitiv von der Diskriminante $-4m$. Es ist nach der Komposition der quadratischen Formen:

$$\psi' = \psi_0 \psi,$$

wenn

$$\begin{aligned} \psi_0 &= \left(2,\ 2,\ \frac{m+1}{2}\right) \quad (m \text{ ungerade}), \\ &= \left(2,\ 0,\ \frac{m}{2}\right) \quad (m \text{ gerade}), \end{aligned}$$

und folglich durchläuft ψ' gleichzeitig mit ψ ein Repräsentantensystem der Diskriminante $-4m$. Es durchläuft aber ω_1 dieselbe Wertreihe wie ω_2, wenn auch in anderer Reihenfolge, und demnach ergibt sich durch Summation der Formel (30):

$$\Pi \frac{f(\omega)}{\sqrt[4]{2}} = 1, \tag{31}$$

wenn sich das Produkt Π auf die Wurzeln mit positiv imaginärem Teil eines vollen Formensystems mit der Diskriminante $-4m$ bezieht.

Wir werden in der Folge der Kürze wegen diese Wertreihe der ω ein vollständiges Wurzelsystem der Diskriminante $-4m$ nennen.

§ 142. Die Normen der Klasseninvarianten $f(\omega)$.

Wir lassen ω ein vollständiges Wurzelsystem der Diskriminante $-4m$ durchlaufen, und setzen voraus, daß in der Form $(A, 2B, C)$, deren Wurzel ω ist, A, C ungerade, A relativ prim zu m sei, worin keine weitere Beschränkung liegt; dann sind nach § 126 die 24sten Potenzen von $f(\omega)$ Klasseninvarianten und ihre Norm ist eine Potenz von 2.

In einer zweiseitigen Klasse gibt es stets einen Repräsentanten von einer der beiden Formen:

$$(A, 0, C), \quad (A, 2B, A),$$

worin A ungerade vorausgesetzt werden kann. Im ersten Falle ist ω rein imaginär und folglich [§ 24, (11)]:

$$f(\omega), \quad f_1(\omega), \quad f_2(\omega)$$

reell und positiv; im zweiten Falle sind ω und $1:\omega$ konjugiert imaginär, folglich:

$$f(\omega) = f\left(-\frac{1}{\omega}\right)$$

reell und

$$f_1(\omega) = f_2\left(-\frac{1}{\omega}\right), \quad f_2(\omega) = f_1\left(-\frac{1}{\omega}\right)$$

konjugiert imaginär, und nach der Formel $f(\omega) f_1(\omega) f_2(\omega) = \sqrt{2}$ ist auch hier $f(\omega)$ positiv.

Wir können also den Repräsentanten $(A, 2B, C)$ immer so gewählt annehmen, daß A und C ungerade sind und daß $f(\omega)$ für eine zweiseitige Klasse reell und positiv wird; repräsentieren

wir ferner zwei entgegengesetzte Klassen durch $(A, \pm 2B, C)$, so sind die entsprechenden Werte von $f(\omega)$ konjugiert imaginär, ihr Produkt daher positiv, und es folgt also nach diesen Bestimmungen, daß das Produkt

$$\Pi f(\omega)$$

einen positiven reellen Wert hat, der eine Potenz von 2 ist. Wir setzen, indem wir mit h die Klassenzahl bezeichnen, diese Potenz $= 2^{h\tau}$, so daß

$$\Pi \frac{f(\omega)}{2^{\tau}} = 1. \tag{1}$$

Es wird unsere Aufgabe sein, diesen Exponenten τ zu bestimmen. Wir schicken aber noch folgende Bemerkung voraus, die dieser Aufgabe ein erhöhtes Interesse verleiht.

Infolge der Gleichung [§ 54, (8)]:

$$f(\omega)^{24} - \gamma_2(\omega) f(\omega)^8 - 16 = 0 \tag{2}$$

ist, wenn ω die Wurzel einer zur Klasse k gehörigen Form der Diskriminante $-4m$ ist, $f(\omega)$ eine ganze algebraische Zahl, und da $f(\omega)^8$ in (2) auch durch $-f_1(\omega)^8$, $-f_2(\omega)^8$ ersetzt werden kann, so sind auch $f_1(\omega)$, $f_2(\omega)$ ganze algebraische Zahlen. Mithin ist es auch

$$\frac{\sqrt{2}}{f(\omega)} = f_1(\omega) f_2(\omega).$$

Ist p eine ungerade Primzahl, von der $-m$ quadratischer Rest ist, und p durch die Formen der Klasse l (der Diskriminante $-4m$) darstellbar, so ist bei passender Bestimmung von c nach § 118:

$$\frac{c + \omega}{p}$$

die Wurzel einer zur komponierten Klasse lk gehörigen Form, und es kann (wenn nicht gerade $p = 3$ ist), c durch 48 teilbar angenommen werden. Setzen wir also:

$$u = f(\omega), \quad v = f\left(\frac{c + \omega}{p}\right),$$

so ist sowohl uv als $2:uv$ eine ganze algebraische Zahl.

Wenn wir daher nach § 74

$$B = (uv)^s + \left(\frac{2}{p}\right) \frac{2^s}{(uv)^s},$$

$$A = \left(\frac{u}{v}\right)^r + \left(\frac{v}{u}\right)^r$$

setzen (wo jetzt A, B natürlich nicht zu verwechseln sind mit den Koeffizienten der quadratischen Form), so ist B eine ganze algebraische Zahl, und nach § 74, (14) ist A die Wurzel einer algebraischen Gleichung, deren Koeffizienten ganze algebraische Zahlen sind. Es ist also A ebenfalls eine ganze algebraische Zahl.

Da aber die beiden Quotienten $u^r : v^r$ und $v^r : u^r$ die Wurzeln der quadratischen Gleichung

$$x^2 - Ax + 1 = 0$$

sind, so folgt, daß

$$\frac{u}{v} \text{ und } \frac{v}{u}$$

ganze Zahlen, und da sie zueinander reziprok sind, Einheiten sind.

Es sind also u und v assoziierte Zahlen.

Da man nun nach § 118 durch wiederholte Kompositionen mit Klassen l (durch die Primzahlen darstellbar sind) von jeder Klasse k zu jeder anderen Klasse k' derselben Diskriminante gelangen kann, und da zwei mit einer dritten assoziierten Zahl untereinander assoziiert sind, so haben wir den Satz:

Setzt man für ω die h Wurzeln der Formen eines Systems von Repräsentanten der Diskriminante $-4m$, so sind die h Zahlen $f(\omega)$ untereinander assoziiert; und daraus nach (1) unmittelbar den merkwürdigen Satz, der sich leicht an allen Beispielen bestätigen läßt:

$f(\omega) : 2^\tau$ ist eine ganze Zahl, und zwar eine Einheit.

1. Die Bestimmung der Exponenten τ ist durch elementare Hilfsmittel möglich, wenn $m \equiv 1$ oder $\equiv 2 \pmod 4$ oder $m \equiv 3 \pmod 8$.

Machen wir in der Gleichung mit ungeraden äußeren Koeffizienten

$$(3) \qquad A\omega^2 + 2B\omega + C = 0$$

mit der Diskriminante $4(B^2 - AC) = -4m$ die Substitution

$$(4) \qquad \omega = \frac{\omega' - 1}{\omega' + 1}, \quad \omega' = -\frac{\omega + 1}{\omega - 1},$$

so erhalten wir die Gleichung

$$(5) \quad \frac{A + 2B + C}{2}\omega'^2 - (A - C)\omega' + \frac{A - 2B + C}{2} = 0,$$

die gleichfalls die Diskriminante $-4m$ hat, und worin, wenn $m \equiv 1$ oder $\equiv 2 \pmod 4$ ist, die beiden äußeren Koeffizienten ungerade sind; denn es ist:

$$\text{für } m \equiv 1 \pmod 4,\quad B \equiv 0 \pmod 2,\quad A + C \equiv 2 \pmod 4,$$
$$\text{für } m \equiv 2 \pmod 4,\quad B \equiv 1 \pmod 2,\quad A + C \equiv 0 \pmod 4.$$

Daraus folgt, daß

$$f(\omega) \text{ und } f\left(\frac{\omega - 1}{\omega + 1}\right),$$

von 24sten Einheitswurzeln abgesehen, dieselbe Wertreihe durchläuft. Denn ersetzt man ω' durch eine äquivalente Zahl, so muß, wenn die äußeren Koeffizienten ungerade bleiben sollen, die Substitution zur ersten oder zweiten Klasse (§ 36) gehören, und daraus folgt aus (4), daß auch ω in eine äquivalente Zahl übergeht. Wenn aber zwei Formen (5) äquivalent sind, so sind auch die entsprechenden Formen (3) äquivalent und umgekehrt.

Demnach ist

$$\Pi f(\omega) f\left(\frac{\omega - 1}{\omega + 1}\right) = 2^{2h\tau},$$

andererseits ist aber [§ 34, (18)]:

$$f(\omega) f\left(\frac{\omega - 1}{\omega + 1}\right) = \sqrt{2},$$

woraus sich ergibt:

(6) $$\tau = \tfrac{1}{4},\quad m \equiv 1, 2 \pmod 4,$$

in Übereinstimmung mit dem Resultat des vorigen Paragraphen [§ 141, (31)].

2. Ist sodann $m \equiv 3 \pmod 8$, so entsprechen einer Wurzel ω' einer Form der Diskriminante $-m$ je drei Wurzeln von Formen der Diskriminante $-4m$:

$$2\omega',\quad \frac{\omega'}{2},\quad \frac{\omega' + 1}{2},$$

und es sind die 24sten Potenzen der Größen:

$$f_1(2\omega') = \frac{\sqrt{2}}{f_2(\omega')},$$
$$f_2\left(\frac{\omega'}{2}\right) = \frac{\sqrt{2}}{f_1(\omega')},$$
$$f_2\left(\frac{\omega' + 1}{2}\right) = \frac{\sqrt{2}}{f(\omega')},$$

deren Produkt $= 2$ ist, Klasseninvariante der Diskriminante $-4D$. Hiernach ist:

$$\Pi f(\omega) = 2^{\frac{1}{3}h},$$

also

(7) $$\tau = \tfrac{1}{3}, \quad m \equiv 3 \pmod 8.$$

3. Für den Fall $m \equiv 7 \pmod 8$ können wir den Wert von τ auf diesem einfachen Wege nicht bestimmen. Es ist dazu die im vorigen Paragraphen abgeleitete Grenzformel erforderlich. Zunächst behandeln wir die beiden Fälle $m \equiv 3 \pmod 4$ gleichmäßig und setzen:

$$\varphi = a x^2 + b x y + c y^2 = (a, b, c),$$

(8) $$b^2 - 4ac = -m,$$

(9) $$S' = \sum^{x,y} \frac{1}{\varphi(x, y)^s},$$

worin x, y alle ganzzahligen Werte, mit Ausnahme der Kombination 0, 0, durchlaufen.

Die Summe S zerlegen wir in vier Partialsummen

$$S'_{00}, \quad S'_{01}, \quad S'_{10}, \quad S'_{11},$$

so daß x, y in S'_{00} nur geradzahlige, in S'_{11} nur ungeradzahlige Werte durchläuft. In S'_{10} durchläuft x die ungeraden, y die geraden Zahlen und umgekehrt in S'_{01}. Dann ist

(10) $$S' + 2S'_{00} = (S'_{01} + S'_{00}) + (S'_{10} + S'_{00}) + (S'_{11} + S'_{00}).$$

Ersetzen wir

in S'_{00}	x, y	durch	$2x, 2y$,
„ $S'_{01} + S'_{00}$	x, y	„	$2x, y$,
„ $S'_{10} + S'_{00}$	x, y	„	$x, 2y$,
„ $S'_{00} + S'_{11}$	x, y	„	$x - y, x + y$,

so sind die neuen x, y keiner weiteren Beschränkung mehr unterworfen, als der, daß nicht beide zugleich verschwinden. Setzen wir daher:

(11) $$\begin{aligned} \varphi &= (a, b, c), \\ \varphi_1 &= (4a, 2b, c), \\ \varphi_2 &= (a, 2b, 4c), \\ \varphi_3 &= (a + b + c, 2(c - a), a - b + c), \end{aligned}$$

so ist

(12) $$\begin{aligned} 4^s S'_{00} &= S', \\ S'_{01} + S'_{00} &= \sum^{x,y} \varphi_1^{-s}, \\ S'_{10} + S'_{00} &= \sum^{x,y} \varphi_2^{-s}, \\ S'_{00} + S'_{11} &= \sum^{x,y} \varphi_3^{-s}. \end{aligned}$$

Wir setzen a als ungerade voraus und lassen φ ein volles Repräsentantensystem der Diskriminante $-m$ durchlaufen. Ist dann $m \equiv 3 \pmod 8$, so ist c ungerade, und φ_1, φ_2, φ_3 durchlaufen zusammen ein Repräsentantensystem der Diskriminante $-4m$. Denn unter den $3h$ Wurzeln dieser Formen

$$\frac{\omega}{2}, \quad 2\omega, \quad 1 - \frac{2}{\omega + 1}$$

kommen nach § 123 keine äquivalenten vor.

Ist dagegen $m \equiv 7 \pmod 8$, so ist c gerade, $\frac{1}{2}\varphi_1$, $\frac{1}{2}\varphi_3$ durchlaufen je ein Repräsentantensystem der Diskriminante $-m$, φ_2 durchläuft ein Repräsentantensystem der Diskriminante $-4m$.

Durchläuft also ψ ein Repräsentantensystem der Diskriminante $-4m$, und setzen wir

$$S = \sum^{x,y} \frac{1}{\psi^s}, \tag{13}$$

so ergibt sich aus (10):

$$\begin{aligned} \left(1 + \frac{2}{4^s}\right) \sum^{\varphi} S' &= \sum^{\psi} S, \quad m \equiv 3 \\ \left(1 + \frac{2}{4^s} - \frac{2}{2^s}\right) \sum^{\varphi} S' &= \sum^{\psi} S, \quad m \equiv 7 \end{aligned} \pmod 8. \tag{14}$$

Setzen wir in den Formeln (29), (30) des vorigen Paragraphen

$$\psi' = 2\varphi, \quad \psi = (A, 2B, C),$$

also:

$$\begin{aligned} A &= a, \\ B &= b - a, \\ C &= 4c - 2b + a, \end{aligned}$$

so ergibt sich:

$$S - \frac{1}{2^s} S' = \frac{2\pi}{\sqrt{m}} \log \frac{f(\omega_1) f(\omega_2)}{\sqrt{2}},$$

und wenn ψ ein Repräsentantensystem der Diskriminante $-4m$ durchläuft, so durchläuft φ dreimal oder nur einmal ein Repräsentantensystem der Diskriminante $-m$, je nachdem $m \equiv 3$ oder $\equiv 7 \pmod 8$ ist. Wir erhalten also, wenn ε in diesen beiden Fällen 3 oder 1 ist:

$$\operatorname*{Lim}_{s=1} \left(\sum^{\psi} S - \frac{\varepsilon}{2^s} \sum^{\varphi} S' \right) = \frac{4\pi}{\sqrt{m}} \log \Pi \frac{f(\omega)}{\sqrt[4]{2}}, \tag{15}$$

worin ω die Wurzeln der Formen ψ durchläuft. Und daraus ergibt sich nach (14):

(16)
$$\lim_{s=1}(4^s+2-3.2^s)\overset{\psi}{\Sigma} S = \frac{24\pi}{\sqrt{m}}\log \Pi \frac{f(\omega)}{\sqrt[4]{2}},\quad m \equiv 3 \pmod 8,$$
$$\lim_{s=1}(4^s+2-3.2^s)\overset{\psi}{\Sigma} S = \frac{8\pi}{\sqrt{m}}\log \Pi \frac{f(\omega)}{\sqrt[4]{2}},\quad m \equiv 7 \pmod 8.$$

Es ist aber [§ 141, (28)]:

$$\lim (s-1)\overset{\psi}{\Sigma} S = \frac{\pi h}{\sqrt{m}},\quad \lim \frac{4^s+2-3.2^s}{s-1} = 2\log 2,$$

also:

(17)
$$\log \Pi \frac{f(\omega)}{\sqrt[3]{2}} = 0,\quad m \equiv 3 \pmod 8,$$
$$\log \Pi \frac{f(\omega)}{\sqrt{2}} = 0,\quad m \equiv 7 \pmod 8.$$

Die erste dieser Formeln gibt das bereits auf andere Weise abgeleitete Resultat; die zweite gibt das neue:

(18) $$\tau = \tfrac{1}{2},\quad m \equiv 7 \pmod 8.$$

4. Es bleibt noch die Bestimmung von τ in dem Falle übrig, wo m durch eine höhere Potenz von 2 teilbar ist. Um auch noch diese Bestimmung auszuführen, sei

(19) $$m = 4m',$$

(20) $$\omega' = \frac{-B+i\sqrt{m}}{A},\quad m' = AC - B^2,$$

also ω' die Wurzel der quadratischen Form $(A, 2B, C)$ der Diskriminante $-m$, worin A und C als **ungerade** vorausgesetzt werden können. Es sind dann

(21) $$\omega_1 = 2\omega',\quad \omega_2 = \frac{\omega'}{2}$$

Wurzeln der Formen

(22) $$(A, 4B, 4C),\quad (4A, 4B, C),$$

und es sind nach § 126, (13) die 24sten Potenzen von

$$f_1(\omega_1) = \frac{\sqrt{2}}{f_2(\omega')},\quad f_2(\omega_2) = \frac{\sqrt{2}}{f_1(\omega')}$$

Klasseninvarianten der Diskriminante $-4m$.

Durchläuft ω' ein vollständiges Wurzelsystem der Diskriminante $-m$, so durchlaufen ω_1 und ω_2 zusammen ein vollständiges Wurzelsystem der Diskriminante $-4m$ (§ 123), und wir erhalten,

wenn ω ein vollständiges Wurzelsystem von Formen mit ungeraden äußeren Koeffizienten durchläuft, mit Benutzung der Formel:

$$f_1(\omega')f_2(\omega')f(\omega') = \sqrt{2},$$

wenn h' die zur Diskriminante $-m'$ gehörige Klassenzahl ist:

$$(23)\quad \Pi f(\omega) = \Pi f_1(\omega_1) f_2(\omega_2) = \frac{2^h}{\Pi f_1(\omega') f_2(\omega')} = \sqrt{2}^{h'}\, \Pi f(\omega'),$$

worin h, h' die Klassenzahlen für die Diskriminanten $-4m$, $-m$ bedeuten. Es ist dann (§ 123):

$$h = 2h'.$$

Sind also wie oben τ, τ' so bestimmt, daß

$$\frac{f(\omega)}{2^\tau},\quad \frac{f(\omega')}{2^{\tau'}}$$

Einheiten werden, so ist

$$\Pi f(\omega) = 2^{h\tau},\quad \Pi f(\omega') = 2^{h'\tau'},$$

und daraus nach (23):

$$(24)\qquad \tau = \frac{\tau'}{2} + \frac{1}{4},$$

eine Formel, die auch noch für $m' = 1$ gilt, wo $h' = h$ und die beiden Werte $2\omega'$ und $\omega' : 2$ äquivalent sind.

Durch wiederholte Anwendung dieser Formel ergibt sich, wenn

$$m = 4^\lambda m'$$

ist, für ein beliebiges positives λ:

$$\tau = \frac{\tau'}{2^\lambda} + \frac{1}{2} - \frac{1}{2^{\lambda+1}}.$$

Fassen wir das hiermit Bewiesene zusammen, so können wir sagen, daß folgende Größen algebraische Einheiten sind:

$$\frac{f(\omega)}{\sqrt[4]{2}},\quad m \equiv 1, 2 \pmod 4,$$

$$\frac{f(\omega)}{\sqrt[3]{2}},\quad m \equiv 3 \pmod 8,$$

$$\frac{f(\omega)}{\sqrt{2}},\quad m \equiv 7 \pmod 8,$$

$$\frac{f(\omega)}{2^{\frac{1}{2}-\frac{1}{2^{\lambda+2}}}}, \quad m = 4^\lambda m', \quad m' \equiv 1, 2 \pmod 4,$$

$$\frac{f(\omega)}{2^{\frac{1}{2}-\frac{1}{3 \cdot 2^{\lambda+1}}}}, \quad m = 4^\lambda m', \quad m' \equiv 4 \pmod 8,$$

$$\frac{f(\omega)}{\sqrt{2}}, \quad m = 4^\lambda m', \quad m' \equiv 7 \pmod 8.$$

§ 143. Partialnormen von $f(\omega)$.

Wir machen von der Grenzformel (30) des § 141 noch eine Anwendung auf die Bestimmung des Produktes

(1) $$\Pi f(\omega),$$

in dem sich das Produktzeichen Π nicht über ein vollständiges Wurzelsystem, sondern nur über die Wurzeln ω der Formenklassen eines Geschlechts erstreckt. Wir beschränken uns dabei aber auf den Fall, daß

(2) $$\varDelta = -4m$$

eine Stammdiskriminante ist, daß also m keinen quadratischen Teiler habe und entweder $\equiv 1$ oder $\equiv 2 \pmod 4$ ist oder, was dasselbe ist,

(3) $$\varDelta \equiv -4 \quad \text{oder} \quad \equiv 8 \pmod{16}.$$

Es sei δ ein von $\varDelta$ und 1 verschiedener Stammteiler von $\varDelta$ und $\chi(\delta, k)$ der diesem Stammteiler entsprechende Charakter der Klasse k.

Ist δ' der zu δ komplementäre Stammteiler zu δ, so ist in diesem Falle

$$\delta\delta' = \varDelta,$$
$$\chi(\delta, k) = \chi(\delta', k),$$

und wir bekommen also alle Geschlechter, wenn wir für δ die ungeraden Stammteiler setzen, was wir hier tun wollen. Es sei nun wie in § 141, (29), (30):

(4) $$\begin{aligned} \psi_0 &= \left(2, 2, \frac{m+1}{2}\right), \quad \left(2, 0, \frac{m}{2}\right), \\ \psi &= (A, 2B, C), \\ \psi' &= \psi_0 \psi. \end{aligned}$$

Sind dann k, k_0, k' die Klassen, zu denen ψ, ψ_0, ψ' gehören, so ist

$$\chi(\delta, k') = \chi(\delta, k_0)\,\chi(\delta, k),$$

also

$$(5)\qquad \begin{aligned}\chi(\delta, k) &= (\delta, A),\\ \chi(\delta, k') &= (\delta, 2)\,(\delta, A).\end{aligned}$$

Ist ω_1 eine Wurzel der Klasse k, so ist ω_2 Wurzel der entgegengesetzten Klasse k^{-1}, in diesen beiden Klassen sind aber die Charaktere $\chi(\delta, k)$ und $\chi(\delta, k^{-1})$ dieselben. Multiplizieren wir daher die Formel § 141, (30) mit $\chi(\delta, k)$ und bilden die Summe über alle Klassen k, so folgt:

$$(6)\qquad \overset{k}{\Sigma}\chi(\delta, k)\left(\overset{x,y}{\Sigma}\frac{1}{\psi^s} - \overset{x,y}{\Sigma}\frac{1}{\psi'^s}\right) = \frac{4\pi}{\sqrt{m}}\overset{k}{\Sigma}\chi(\delta, k)\log\frac{f(\omega)}{\sqrt[4]{2}},$$

und wegen (5) kann man für die linke Seite schreiben:

$$[1 - (\delta, 2)]\overset{k}{\Sigma}\frac{\chi(\delta, k)}{1}\overset{x,y}{\Sigma}\frac{1}{\psi^s}.$$

Demnach haben wir:

$$(7)\qquad \begin{aligned}(\delta, 2) = +1:&\quad \frac{2\pi}{\sqrt{m}}\overset{k}{\Sigma}\chi(\delta, k)\log\frac{f(\omega)}{\sqrt[4]{2}} = 0,\\ (\delta, 2) = -1:&\quad \frac{2\pi}{\sqrt{m}}\overset{k}{\Sigma}\chi(\delta, k)\log\frac{f(\omega)}{\sqrt[4]{2}} = \overset{k}{\Sigma}\chi(\delta, k)\overset{x,y}{\Sigma}\frac{1}{\psi^s},\end{aligned}$$

wobei rechts der Grenzwert für $s = 1$ zu nehmen ist.

In § 113 haben wir die Formel bewiesen:

$$(8)\qquad \overset{k}{\Sigma}\chi(\delta, k)\overset{x,y}{\Sigma}\frac{1}{\psi^s} = \Sigma\frac{(\delta, n)}{n^s}\Sigma\frac{(\delta', n)}{n^s}.$$

Wenn wir mit $K(\delta)$ die Klassenzahl für die Diskriminante δ bezeichnen, so ist, wie in § 112, (8) bewiesen ist:

$$(9)\qquad \begin{aligned}\sum^{n}\frac{(\delta, n)}{n} &= \frac{\pi}{\sqrt{-\delta}}\,K(\delta) &\qquad \delta < 0,\\ \sum^{n}\frac{(\delta, n)}{n} &= \frac{\log\varepsilon}{\sqrt{\delta}}\,K(\delta) &\qquad \delta > 0,\end{aligned}$$

worin die Quadratwurzeln positiv zu nehmen sind, und

$$\varepsilon = \frac{T + U\sqrt{\delta}}{2}$$

die fundamentale positive Einheit des quadratischen Körpers mit der Grundzahl δ ist. Für die beiden Ausnahmefälle $\delta = -3$, $\delta = -4$ gelten diese Formeln, wenn man unter K nicht die

Klassenzahl selbst, sondern den dritten Teil oder die Hälfte davon versteht.

Nun ist δ' immer gerade und von entgegengesetztem Vorzeichen wie δ, und $4m = -\delta\delta'$; danach ergeben sich aus (7) die Formeln:

$$(10)\quad 2\sum^{k} \chi(\delta, k) \log \frac{f(\omega)}{\sqrt[4]{2}} = 0, \qquad \delta \equiv 1 \pmod 8,$$
$$= K(\delta) K(\delta') \log \varepsilon, \quad \delta \equiv 5 \pmod 8,$$

worin

$$(11)\qquad \varepsilon = \frac{T + U\sqrt{\delta}}{2}, \quad \delta > 0 \equiv 1 \pmod 8,$$
$$= \frac{T + U\sqrt{\delta'}}{2}, \quad \delta < 0 \equiv 5 \pmod 8$$

zu setzen ist. Die erste der Formeln (10) gilt auch noch für $\delta = 1$.

Da nun für alle Klassen eines Geschlechts und für jedes δ der Charakter $\chi(\delta, k)$ denselben Wert hat, so sind durch (10) und (11) die Produkte (1) bestimmt. Denn es ist nach § 113

$$\sum^{\delta} \chi(\delta, k) = 0,$$

außer wenn k die Hauptklasse ist, und für diese ist die Summe gleich der Anzahl g der Geschlechter. Man erhält z. B. für die Wurzeln ω des Hauptgeschlechts

$$\left(\Pi \frac{f(\omega)}{\sqrt[4]{2}}\right)^{2g} = \Pi\, \varepsilon^{K(\delta) K(\delta')},$$

worin g die Anzahl der Geschlechter bedeutet, und das Produkt links über alle Wurzeln ω des Hauptgeschlechts, das Produkt rechts über alle Stammteiler δ von Δ, die $\equiv 5 \pmod 8$ sind, auszudehnen ist.

Um das Produkt der Klasseninvarianten für ein anderes als das Hauptgeschlecht zu bilden, hat man die Formel (8) vor der Summation mit $\chi(\delta, k^{-1})$ zu multiplizieren, wenn k eine Klasse des betreffenden Geschlechts bedeutet.

Die Anwendung der Formel (10) verlangt die Kenntnis der Klassenzahlen positiver und negativer Diskriminanten und der Zahlen T, U. Die Klassenzahlen sind in weitem Umfange von Gauss berechnet und aus seinem Nachlaß im zweiten Bande der Werke, S. 450 bis 476, veröffentlicht. Für die Lösungen T, U der Pellschen Gleichung enthält Legendres „Theorie des nombres" oder auch der „Canon Pellianus" von Degen eine Tabelle.

Es existieren 63 negative Diskriminanten von der Eigenschaft, daß in jedem Geschlecht nur eine Klasse enthalten ist; daß es nicht mehr gibt, selbst daß die Zahl nur eine endliche ist, kann freilich bis jetzt nur durch Induktion geschlossen, nicht bewiesen werden. Die Mehrzahl dieser Diskriminanten, die bereits in § 139 zusammengestellt sind, ist $\equiv 1, 2 \pmod 4$ und ohne quadratischen Teiler oder $\equiv 8 \pmod{16}$.

Für die ersteren lassen sich die Klasseninvarianten nach der Formel (10) vollständig berechnen, und eine ähnliche Formel, auf deren Bildung wir hier nicht eingehen wollen, führt auch für die durch 8 teilbaren Diskriminanten zum Ziel.

Für die vereinzelten Diskriminanten dieser Art, die hierher nicht passen, lassen sich die Klasseninvarianten $f(\omega)$ nach einer der anderen Methoden berechnen[1]).

Um an einem einfachen, leicht zu übersehenden Beispiele die Rechnung durchzuführen, wählen wir $m = 105 = 3.\ 5.\ 7.$ Wenn wir die Werte von δ, die $\equiv 1 \pmod 8$ sind, weglassen, da diese in der Summe der Formeln (10) keinen Beitrag geben, so haben wir:

$$\begin{array}{lllll} \delta = & -3, & 5, & 21, & -35, \\ \delta' = & 140, & -84, & -20, & 12 \end{array}$$

zu setzen und erhalten, da $g = 8$ ist:

$$\begin{aligned} 16 \log \frac{f(\sqrt{-105})}{\sqrt[4]{2}} = {} & K(-3)\ K(140)\ \log \frac{T + U\sqrt{140}}{2}, \\ & + K(5)\quad K(-84) \log \frac{T + U\sqrt{84}}{2}, \\ & + K(21)\quad K(-20) \log \frac{T + U\sqrt{20}}{2}, \\ & + K(-35) K(12)\quad \log \frac{T + U\sqrt{12}}{2}. \end{aligned}$$

---

[1]) Vgl. des Verfassers Abhandlung: „Zur komplexen Multiplikation elliptischer Funktionen". Mathematische Annalen, Bd. 23. Ich mache hier auf einen Fehler in der Gaussschen Tafel aufmerksam, den ich bei Gelegenheit dieser Rechnungen gefunden habe: Gauss' Werke, Bd. II, S. 475 muß die positive Determinante 136 die Bezeichnung IV, 2, nicht IV, 1 haben.

Es ist aber

$$K(-3) = \tfrac{1}{3},\ K(-84) = 4,\ K(-20) = 2,\ K(-35) = 2,$$
$$K(+140) = 4,\ K(5) = 1,\ K(21) = 2,\ K(12) = 2$$ [1],

wie man aus den Gaussschen Tafeln oder hier auch leicht durch direkte Abzählung findet.

Ferner ist nach den Legendreschen oder Degenschen Tafeln:

$$\log\left(\frac{T+\sqrt{140}\,U}{2}\right) = \log(6+\sqrt{35}) = \log\frac{(\sqrt{5}+\sqrt{7})^2}{2},$$

$$\log\left(\frac{T+\sqrt{5}\,U}{2}\right) = \log\left(\frac{1+\sqrt{5}}{2}\right)^2 = \tfrac{2}{3}\log(2+\sqrt{5}),$$

$$\log\frac{T+\sqrt{21}\,U}{2} = \log\frac{5+\sqrt{21}}{2} = \tfrac{1}{3}\log(55+12\sqrt{21})$$
$$= \log\left(\frac{\sqrt{3}+\sqrt{7}}{2}\right)^2,$$

$$\log\left(\frac{T+\sqrt{12}\,U}{2}\right) = \log(2+\sqrt{3}),$$

und daraus erhält man:

$$\left(\frac{f(\sqrt{-105})}{\sqrt[4]{2}}\right)^{12} = (2+\sqrt{5})^2(55+12\sqrt{21})(6+\sqrt{35})(2+\sqrt{3})^3,$$

oder was damit gleichbedeutend ist:

$$\sqrt{2}^{13} f(\sqrt{-105})^6 = (1+\sqrt{5})^3(\sqrt{3}+\sqrt{7})^3(\sqrt{5}+\sqrt{7})(1+\sqrt{3})^3.$$

§ 144. Berechnung einiger weiterer Klasseninvarianten.

Nächst den Diskriminanten, bei denen in jedem Geschlecht nur eine Formenklasse vorkommt, die wir im vorhergehenden Paragraphen betrachtet haben, geben die einfachsten Resultate die, welche in jedem Geschlecht zwei Formenklassen enthalten, und unter diesen wieder die, bei denen nur zwei Geschlechter vorkommen. Die Klasseninvarianten für diese Diskriminanten $-4m$ sind die Wurzeln quadratischer Gleichungen, deren Koeffizienten nur eine Quadratwurzel enthalten. Wir setzen wieder Stammdiskriminanten voraus, und erhalten nach der Gaussschen Tafel die folgenden Werte von m:

[1] Nach Gaussscher Bezeichnung sind die Klassenzahlen zweiter Art zu nehmen.

$$m = 14,\ 34,\ 46,\ 82,\ 142 \equiv \pm 2 \pmod{16},$$
$$m = 17,\ 49,\ 73,\ 97,\ 193 \equiv 1 \pmod{8}.$$

Die Formenklassen des Hauptgeschlechts können in diesen Fällen repräsentiert werden für ein gerades m durch

(1) $$(1,\ 0,\ m),\quad \left(2,\ 0,\ \frac{m}{2}\right),$$

für ein ungerades m durch

(2) $$(1,\ 0,\ m),\quad \left(2,\ 1,\ \frac{m+1}{2}\right),$$

von denen die letztere äquivalent ist mit

(3) $$\left(\frac{m+1}{2},\ \frac{m-1}{2},\ \frac{m+1}{2}\right).$$

Für die Formen (1) sind nach § 127, 6. die Klasseninvarianten

$$\frac{f_1(\sqrt{-m})^2}{\sqrt{2}} \quad \text{und} \quad \frac{1}{\sqrt{2}} f_2\left(\frac{\sqrt{-m}}{2}\right)^2 = \frac{\sqrt{2}}{f_1(\sqrt{-m})^2} \quad (\S\ 34)$$

und für die Formen (2), (3) (§ 127, 3.)

$$\frac{f(\sqrt{-m})^2}{\sqrt{2}} \quad \text{und} \quad \frac{1}{\sqrt{2}} f\left(\frac{1+\sqrt{-m}}{1-\sqrt{-m}}\right)^2 = \frac{\sqrt{2}}{f(\sqrt{-m})^2},$$

und nach § 142 sind dies ganze algebraische Zahlen.

Setzen wir also, entsprechend den beiden Fällen:

(4) $$\sqrt{2}\,x = f_1(\sqrt{-m})^2,\quad f(\sqrt{-m})^2,$$

so ist

$$x + \frac{1}{x}$$

eine ganze algebraische Zahl, die nur eine Quadratwurzel enthält, und aus § 138 erhalten wir Aufschluß, welche Quadratwurzel darin vorkommt.

Es ist $\sqrt{2}$, wenn $m \equiv 6 \pmod 8$ ist, also für $m = 14,\ 46,\ 142$, $\sqrt{\frac{m}{2}}$, wenn $m \equiv 2 \pmod 8$ ist, also für $m = 34,\ 82$, ferner $\sqrt{m}$ im Fall eines ungeraden m (mit Ausnahme von $m = 49$, wo $\sqrt{7}$ an die Stelle tritt).

Setzen wir also

(5) $$x + \frac{1}{x} = a + b\sqrt{p},$$

so sind a, b rationale Zahlen, die höchstens den Nenner 2 haben. Es müssen aber auch a und b positiv sein. Denn ändern wir in (5) das Vorzeichen von $\sqrt{p}$, so entsteht eine andere quadratische

Gleichung, deren Wurzeln die zum zweiten Geschlecht gehörigen Klasseninvarianten sind, und die daher konjugiert imaginär sind, während die Wurzeln von (5) reell sind. Daraus ergibt sich die Größenbestimmung:

$$(a + b\sqrt{p})^2 > 4 > (a - b\sqrt{p})^2;$$

also müssen a und b gleiches Zeichen haben. Da aber x nach (4) positiv ist, so müssen a und b beide positiv sein.

Um a und b wirklich zu finden, braucht man nur den Ausdruck auf der linken Seite von (5) nach (4) auf wenige Dezimalen zu berechnen, wobei es weitaus hinreichend ist,

$$f(\sqrt{-m}) = f_1(\sqrt{-m}) = e^{\frac{\pi\sqrt{m}}{24}}$$

zu setzen, und die so gefundenen Dezimalen mit den Dezimalen von $\sqrt{p}$ zu vergleichen, um alsbald b und sodann a zu erhalten. Die Rechnung ist überaus einfach und gibt folgende Resultate:

$$m = 14, \quad x + \frac{1}{x} = 1 + \sqrt{2},$$

$$m = 17, \quad x + \frac{1}{x} = \frac{1 + \sqrt{17}}{2},$$

$$m = 34, \quad x + \frac{1}{x} = \frac{3 + \sqrt{17}}{2},$$

$$m = 46, \quad x + \frac{1}{x} = 3 + \sqrt{2},$$

$$m = 49, \quad x + \frac{1}{x} = 2 + \sqrt{7},$$

$$m = 73, \quad x + \frac{1}{x} = \frac{5 + \sqrt{73}}{2},$$

$$m = 82, \quad x + \frac{1}{x} = \frac{15 + \sqrt{41}}{2},$$

$$m = 97, \quad x + \frac{1}{x} = \frac{9 + \sqrt{97}}{2},$$

$$m = 142, \quad x + \frac{1}{x} = 9 + 5\sqrt{2},$$

$$m = 193, \quad x + \frac{1}{x} = 13 + \sqrt{193}.$$

Zweiundzwanzigster Abschnitt.

Cayleys Entwickelung der Modulfunktionen.

§ 145. Grenzwerte für $s = 1$.

In diesem Abschnitt soll eine funktionentheoretische Anwendung der Grenzformel gegeben werden. Es bedeutet also hier ω nicht eine quadratische Irrationalzahl, sondern eine Variable mit positiv imaginärem Bestandteil. Die Modulfunktionen gehören zu den Funktionen mit natürlichen Grenzen, d. h. wenn man sich der Grenze der Konvergenz nähert, so liegen auf dieser Grenze, hier also auf der Achse der reellen ω, die singulären Punkte überall dicht, so daß man diese Funktionen über diese Grenze hinaus nicht analytisch fortsetzen kann. Cayley hat in seinen letzten Untersuchungen Entwickelungen der Modulfunktionen gegeben, die darum merkwürdig sind, weil sie das Verhalten der Funktionen bei der Annäherung an die Grenze augenfällig machen. Der Schlüssel zu diesen Entwickelungen ist die Grenzformel § 141, (27)[1].

Wenn man in dieser Formel:

$$(1)\qquad \operatorname*{Lim}_{s=1} \sum^{x,y} \frac{1}{(Ax^2+2Bxy+Cy^2)^s} - \frac{\pi}{(s-1)\sqrt{m}}$$

$$= -\frac{2\pi\Gamma'(1)}{\sqrt{m}} + \frac{\pi}{\sqrt{m}}\log\frac{A}{4m} - \frac{2\pi}{\sqrt{m}}\log \eta(\omega_1), \eta(\omega_2),$$

$$\omega_1 = \frac{B+i\sqrt{m}}{A}, \quad \omega_2 = \frac{-B+i\sqrt{m}}{A},$$

$$(2)\qquad \omega_1 = \alpha+\beta i, \quad \omega_2 = -\alpha+\beta i, \quad \beta > 0$$

[1]) Die erste Cayleysche Arbeit findet sich in dem Comptes Rendus der Pariser Akademie von 1893, Bd. 161. Weiteres in einem Briefwechsel mit dem Verfasser dieses Buches, der im 47. Bande der mathematischen Annalen veröffentlicht ist.

setzt, so ergibt sich

$$A = 1, \quad B = \alpha, \quad C = \alpha^2 + \beta^2, \quad m = \beta^2,$$

und die Formel 1 ergibt:

$$(3) \quad \sum^{x,y} \frac{1}{[(x - \alpha y)^2 + \beta^2 y^2]^s} = \sum^{x,y} \frac{1}{(x + \omega_1 y)^s (x - \omega_2 y)^s}$$
$$= \frac{\pi}{(s-1)\beta} - \frac{2\pi \Gamma'(1)}{\beta} - \frac{\pi}{\beta} \log 4\beta^2 - \frac{2\pi}{\beta} \log \eta(\omega_1)\eta(\omega_2).$$

Das Zeichen Lim ist hier der Kürze wegen weggelassen.

Wir setzen

$$(4) \qquad S = \sum^{x,y} \frac{1}{[(x - \alpha y)^2 + \beta^2 y^2]^s},$$

worin x, y alle ganzzahligen Werte mit Ausnahme der Kombination 0,0 durchlaufen. S ist eine unbedingt konvergente Reihe, solange $s > 1$ ist.

Nun teilen wir die Glieder von S in drei Arten ein, je nachdem die x, y gerade oder ungerade sind, und setzen

$$(5) \qquad \begin{aligned} S_0 &= \sum^{x,y} \frac{1}{[(x - \alpha y)^2 + \beta^2 y^2]^s}, \quad x \equiv y \pmod 2, \\ S_1 &= \sum^{x,y} \frac{1}{[(x - \alpha y)^2 + \beta^2 y^2]^s}, \quad x \equiv 0 \pmod 2, \\ S_2 &= \sum^{x,y} \frac{1}{[(x - \alpha y)^2 + \beta^2 y^2]^s}, \quad y \equiv 0 \pmod 2. \end{aligned}$$

In S_0 sind also die Zahlen x, y entweder beide gerade oder beide ungerade, in S_1 durchläuft x die geraden, y alle ganzen Zahlen, in S_2 ist y gerade, x beliebig. Betrachtet man die Summe $S_0 + S_1 + S_2$, so kommen darin alle Glieder von S vor, und zwar die Glieder dreimal, in denen x und y beide gerade sind. Hebt man in der Summe dieser Glieder den Faktor 4^{-s} heraus, so bleibt S selbst übrig, und es ergibt sich also:

$$(6) \qquad S_0 + S_1 + S_2 = \left(1 + \frac{2}{4^s}\right) S.$$

Geht man zur Grenze $s = 1$ über, so hat man zu setzen

$$(7) \qquad \frac{1}{4^s} = \frac{1}{4} - \frac{s-1}{2} \log 2 \ldots,$$

und erhält aus (3) die für $s = 1$ gültige Formel:

$$(8) \qquad S_0 + S_1 + S_2 = \frac{3}{2} S - \frac{\pi}{\beta} \log 2.$$

Ersetzen wir α und β in S durch 2α und 2β, so hat das denselben Erfolg, als wenn wir y durch $2y$ ersetzen, d. h. es geht S in S_2 über, und demnach erhalten wir aus (3):

$$(9) \qquad 2 S_2 = \frac{\pi}{(s-1)\beta} - \frac{2\pi\Gamma'(1)}{\beta} - \frac{\pi}{\beta}\log 4\beta^2 - \frac{2\pi}{\beta}\log 2\eta(2\omega_1)\,\eta(2\omega_2).$$

Ersetzt man α, β durch $\frac{1}{2}\alpha$, $\frac{1}{2}\beta$ und multipliziert mit 4^{-s}, so ist der Erfolg derselbe, als ob man x durch $2x$ ersetzt hätte, und man erhält S_1. Also nach (3) mit Rücksicht auf (7):

$$(10) \qquad 2 S_1 = \frac{\pi}{(s-1)\beta} - \frac{2\pi\Gamma'(1)}{\beta} - \frac{\pi}{\beta}\log 4\beta^2 - \frac{2\pi}{\beta}\log \eta\left(\frac{\omega_1}{2}\right)\eta\left(\frac{\omega_2}{2}\right).$$

Ersetzt man endlich α, β durch $\frac{1}{2}(\alpha+1)$, $\frac{1}{2}\beta$ und dann $2x-y$ durch x, so ergibt sich in gleicher Weise:

$$(11) \qquad 2 S_0 = \frac{\pi}{(s-1)\beta} - \frac{2\pi\Gamma'(1)}{\beta} - \frac{\pi}{\beta}\log 4\beta^2 - \frac{2\pi}{\beta}\log \eta\left(\frac{1+\omega_1}{2}\right)\eta\left(\frac{-1+\omega_2}{2}\right),$$

und demnach mit Rücksicht auf die Formeln [§ 34, (9)]:

$$f(\omega) = e^{-\frac{\pi i}{24}}\,\frac{\eta\left(\frac{\omega+1}{2}\right)}{\eta(\omega)} = e^{\frac{\pi i}{24}}\,\frac{\eta\left(\frac{\omega-1}{2}\right)}{\eta(\omega)},$$

$$f_1(\omega) = \frac{\eta\left(\frac{\omega}{2}\right)}{\eta(\omega)}, \qquad f_2(\omega) = \sqrt{2}\,\frac{\eta(2\omega)}{\eta(\omega)},$$

indem man die Formeln (9), (10), (11) von (3) subtrahiert:

$$S - 2S_0 = \frac{2\pi}{\beta}\log f(\omega_1)\,f(\omega_2),$$

$$S - 2S_1 = \frac{2\pi}{\beta}\log f_1(\omega_1)\,f_1(\omega_2),$$

$$S - 2S_2 = \frac{2\pi}{\beta}\log f_2(\omega_1)\,f_2(\omega_2),$$

woraus sich durch Addition nach § 34, (11) die Relation (8) wieder ergibt.

In der Differenz $2S_0 - S$ kommen nun genau dieselben Glieder vor wie in S, nur erhalten die, in denen $x + y$ ungerade ist, das negative Zeichen, und wir können daher auch setzen:

$$\frac{-2\pi}{\beta}\log f(\omega_1)\, f(\omega_2) = \operatorname*{Lim}_{s=1} \sum \frac{(-1)^{x+y}}{[(x-\alpha y)^2 + \beta^2 y^2]^s},$$

$$(12)\qquad \frac{-2\pi}{\beta}\log f_1(\omega_1)\, f_1(\omega_2) = \operatorname*{Lim}_{s=1} \sum \frac{(-1)^{x}}{[(x-\alpha y)^2 + \beta^2 y^2]^s},$$

$$\frac{-2\pi}{\beta}\log f_2(\omega_1)\, f_2(\omega_2) = \operatorname*{Lim}_{s=1} \sum \frac{(-1)^{y}}{[(x-\alpha y)^2 + \beta^2 y^2]^s},$$

worin nun x, y alle ganzzahligen Wertpaare mit Ausnahme von 0,0 annehmen. Diese drei Formeln lassen sich nach § 34, (13), (14) aus einer von ihnen ableiten, z. B. indem man in der zweiten

$$\omega_1,\ \omega_2 \quad \text{durch} \quad \omega_1 + 1,\quad \omega_2 - 1,$$
$$\text{und durch} \quad \frac{-1}{\omega_1},\quad \frac{-1}{\omega_2},$$

(13) also

$$\alpha,\ \beta \quad \text{durch} \quad \alpha + 1,\quad \beta,$$
$$\text{und durch} \quad \frac{-\alpha}{\alpha^2+\beta^2},\quad \frac{\beta}{\alpha^2+\beta^2}$$

ersetzt.

§ 146. Ein Satz über Reihenkonvergenz.

Wollte man in den Ausdrücken (12), § 145 die Zeichen Lim und Σ miteinander vertauschen, also ohne weiteres unter dem Summenzeichen $s = 1$ setzen, so würde man keine unbedingt konvergente Reihen erhalten, und es muß also untersucht werden, in welchem Sinne diese Formeln dann noch gültig bleiben.

Um diese Untersuchung durchzuführen, wollen wir zunächst einen allgemeinen Satz aus der Reihenlehre ableiten, der eine Verschärfung des Satzes Bd. II, § 196, 3. ist. Es sei

$$(1)\qquad \mu_1 \gtreqless \mu_2 \gtreqless \mu_3 \gtreqless \mu_4 \cdots$$

eine Reihe von unendlich vielen positiven Zahlen, und $Z(t)$ bedeute die Anzahl dieser Zahlen, die nicht größer als t sind. Dieses $Z(t)$ soll für jedes t einen endlichen Wert haben, woraus dann folgt, daß die μ_n mit n ins unendliche wachsen. Wir wollen aber noch weiter voraussetzen, daß

$$(2)\qquad \frac{Z(t)}{t} = a + \frac{\theta}{\sqrt{t}}$$

sei, worin a eine konstante (unabhängig von t), und θ eine Funktion von t, die in endlichen Grenzen eingeschlossen bleibt.

Nehmen wir zunächst an, die μ_n seien alle voneinander verschieden, so ist $Z(\mu_n) = n$, und aus (2) folgt:

$$(3) \qquad \frac{n}{\mu_n} = a + \frac{\theta}{\sqrt{\mu_n}};$$

daraus folgt, daß $n:\mu_n$ endlich bleibt, und folglich mit veränderter Bedeutung von θ:

$$\frac{n}{\mu_n} = a + \frac{\theta}{\sqrt{n}},$$

oder, nach dem binomischen Satz, für irgend ein positives s:

$$(4) \qquad \frac{n^s}{\mu_n^s} = a^s\left(1 + \frac{\theta}{\sqrt{n}}\right),$$

worin alle die mit θ bezeichneten Größen endliche Werte haben.

Diese Formeln gelten aber auch noch, wenn unter den μ_n gleiche vorkommen. Denn seien etwa (wie in Bd. II, § 196, 3.)

$$\mu_{m+1}, \mu_{m+2}, \ldots, \mu_{m+l} = \mu_n$$

einander gleich und

$$m < n \leqq m + l,$$

so ist

$$Z(\mu_n - 0) = m, \quad Z(\mu_n) = m + l,$$

$$\frac{Z(\mu_n - 0)}{\mu_n} < \frac{n}{\mu_n} \leqq \frac{Z(\mu_n)}{\mu_n},$$

$$a + \frac{\theta'}{\sqrt{\mu_n}} < \frac{n}{\mu_n} < a + \frac{\theta}{\sqrt{\mu_n}},$$

woraus (3) folgt und (4) wie oben abgeleitet werden kann.

Der Satz, den wir beweisen wollen, lautet so:

Es sei $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ eine unendliche Reihe positiver oder negativer, aber endlicher Größen und

$$(5) \qquad \varepsilon_1 + \varepsilon_2 + \cdots + \varepsilon_n = \gamma_n \sqrt{n},$$

so beschaffen, daß γ_n dem absoluten Werte nach unter einer endlichen Konstanten bleibt.

Dann ist

$$(6) \qquad \sigma = \frac{\varepsilon_1}{\mu_1^s} + \frac{\varepsilon_2}{\mu_2^s} + \frac{\varepsilon_3}{\mu_3^s} + \cdots$$

konvergent und eine stetige Funktion von s, so lange

$$s > \tfrac{1}{2}$$

ist.

Wegen (4) braucht dieser Satz nur bewiesen zu werden für $\mu_n = n$, weil die Reihe $\Sigma\, \varepsilon_n\, 0/n^{s+\frac{1}{2}}$ unbedingt konvergiert und also nach bekannten elementaren Sätzen diese Eigenschaft hat.

Setzen wir also

$$(7) \qquad \sigma = \frac{\varepsilon_1}{1^s} + \frac{\varepsilon_2}{2^s} + \frac{\varepsilon_3}{2^s} + \cdots$$

und nach (5) $\varepsilon_n = \gamma_n \sqrt{n} - \gamma_{n-1}\sqrt{n-1}$, so wird

$$(8) \qquad \sigma = \frac{\varepsilon_1}{1^s} + \gamma_2\sqrt{2}\left(\frac{1}{2} - \frac{1}{3^s}\right) + \gamma_3\sqrt{3}\left(\frac{1}{3^s} - \frac{1}{4^s}\right) + \cdots$$

Da nun für ein unendlich großes n

$$\sqrt{n}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) = \frac{s}{n^{s+\frac{1}{2}}}$$

ist, so ist die Reihe (8) unbedingt konvergent, solange $s > \frac{1}{2}$ ist, und daraus folgt auch für diese Reihe unsere Behauptung nach denselben elementaren Sätzen.

§ 147. Entwickelung von f, f_1, f_2.

Die Reihen (12), § 145 sind nun in diesem Falle. Betrachten wir z. B. die zweite von ihnen, aus denen, wie wir gesehen haben, die anderen hergeleitet werden können, und setzen für $\mu_1, \mu_2, \mu_3, \ldots$ die der Größe nach geordneten Werte der Funktion

$$(1) \qquad (x - \alpha y)^2 + \beta^2 y^2 = n.$$

Wir nehmen xy als rechtwinkelige Koordinaten in der Ebene und überlagern die Ebene mit zwei Gittern, indem wir in dem einen Gitter für die x die geraden, in dem anderen die ungeraden ganzen Zahlen setzen.

Die Anzahl der Gitterpunkte, die im Innern der Ellipse (1) oder auf ihrer Peripherie liegen, für die daher $\mu_n \leqq n$ ist, bezeichnen wir für die beiden Arten mit $Z^0(n)$, $Z^1(n)$.

Setzen wir

$$x = \xi\sqrt{n}, \qquad y = \eta\sqrt{n},$$

so geht (1) über in

$$(2) \qquad (\xi - \alpha\eta)^2 + \beta^2\eta^2 = 1,$$

und der Flächeninhalt dieser Ellipse ist π/β, und nach Bd. II, § 194, 1.:

$$(3)\qquad \frac{Z^0(t)}{t} = \frac{\pi}{2\beta} + \frac{\gamma^0}{\sqrt{t}},\qquad \frac{Z^1(t)}{t} = \frac{\pi}{2\beta} + \frac{\gamma^1}{\sqrt{t}},$$

worin γ^0 und γ^1 für $t = \infty$ endlich bleiben. Der Faktor $\frac{1}{2}$ bei $\pi/2\beta$ kommt daher, daß hier die Gittermaschen Rechtecke vom Inhalt 2 sind. Dies ist aber in Übereinstimmung mit der Formel § 146, (2).

Aus (3) ergibt sich

$$(4)\qquad Z^0(t) - Z^1(t) = \gamma\sqrt{t},$$

worin γ gleichfalls endlich bleibt.

Nun können wir die in der Formel (12), § 145 vorkommende Summe

$$\sigma = \sum \frac{(-1)^x}{[(x-\alpha y)^2 + \beta^2 y^2]^s}$$

so schreiben:

$$\sigma = \frac{\varepsilon_1}{\mu_1^s} + \frac{\varepsilon_2}{\mu_2^s} + \frac{\varepsilon_3}{\mu_3^s} + \cdots,$$

worin die $\varepsilon_1, \varepsilon_2, \varepsilon_3, \ldots$ nur die Werte ± 1 haben und

$$(5)\qquad \varepsilon_1 + \varepsilon_2 + \varepsilon_3 + \cdots + \varepsilon_n = Z^0(n) - Z^1(n), \quad = \gamma\sqrt{n}.$$

Damit sind die Voraussetzungen unseres Satzes § 146 erfüllt.

Es ist also σ für $s > \frac{1}{2}$ eine stetige Funktion von s, also insbesondere auch für $s = 1$, und wir erhalten aus § 145, (12):

$$(6)\qquad \begin{aligned} -\frac{2\pi}{\beta}\log f(\omega_1)\, f(\omega_2) &= \sum \frac{(-1)^{x+y}}{(x-\alpha y)^2 + \beta^2 y^2},\\ -\frac{2\pi}{\beta}\log f_1(\omega_1)\, f_1(\omega_2) &= \sum \frac{(-1)^{x}}{(x-\alpha y)^2 + \beta^2 y^2},\\ -\frac{2\pi}{\beta}\log f_2(\omega_1)\, f_2(\omega_2) &= \sum \frac{(-1)^{y}}{(x-\alpha y)^2 + \beta^2 y^2}. \end{aligned}$$

Man kann diese Formeln auch noch anders darstellen. Wir führen die Bezeichnung ein:

$$(7)\qquad \sum \frac{1}{(x-\alpha y)^2 + \beta^2 y^2} \begin{aligned} &= S_{00} : x \text{ gerade}, \; y \text{ gerade},\\ &= S_{01} : x \text{ gerade}, \; y \text{ ungerade},\\ &= S_{10} : x \text{ ungerade}, \; y \text{ gerade},\\ &= S_{11} : x \text{ ungerade}, \; y \text{ ungerade}. \end{aligned}$$

Dann ist

$$\frac{2\pi}{\beta}\log f(\omega_1)\, f(\omega_2) = -S_{00} + S_{10} + S_{01} - S_{11},$$

(8) $$\frac{2\pi}{\beta}\log f_1(\omega_1)\, f_1(\omega_2) = -S_{00} + S_{10} - S_{01} + S_{11},$$

$$\frac{2\pi}{\beta}\log f_2(\omega_1)\, f_2(\omega_2) = -S_{00} - S_{10} + S_{01} + S_{11},$$

woraus durch Addition:

$$\frac{2\pi}{\beta}\log 2 = -3\, S_{00} + S_{10} + S_{01} + S_{11},$$

und wenn man hierdurch S_{00} eliminierte:

$$\frac{2\pi}{\beta}\log f(\omega_1)\, f(\omega_2) = \frac{2\pi}{3\beta}\log 2 + \tfrac{2}{3} S_{10} + \tfrac{2}{3} S_{01} - \tfrac{4}{3} S_{11},$$

(9) $$\frac{2\pi}{\beta}\log f_1(\omega_1)\, f_1(\omega_2) = \frac{2\pi}{3\beta}\log 2 + \tfrac{2}{3} S_{10} - \tfrac{4}{3} S_{01} + \tfrac{2}{3} S_{11};$$

$$\frac{2\pi}{\beta}\log f_2(\omega_1)\, f_2(\omega_2) = \frac{2\pi}{3\beta}\log 2 - \tfrac{4}{3} S_{10} + \tfrac{2}{3} S_{01} + \tfrac{2}{3} S_{11}.$$

Diese Summen sind aber so zu verstehen, daß in allen zugleich

$$(x - \alpha y)^2 + \beta^2 y^2 < n$$

sein soll, und dann n ins Unendliche wächst. Jede einzelne Summe S wird dann unendlich, aber ihre Verbindungen, wie sie in diesen Formeln vorkommen, erhalten endliche Grenzwerte.

Wir wollen noch mit S'_{01}, S'_{10}, S'_{11} die Summen bezeichnen, die denselben Ausdruck haben wie S_{01}, S_{10}, S_{11} nach (6), nur mit dem Unterschied, daß x und y keinen gemeinschaftlichen Teiler haben sollen.

Setzen wir

$$S_{10} + S_{01} - 2\, S_{11} = T_n,$$
$$(x - \alpha y)^2 + \beta^2 y^2 < n,$$
$$\lim_{n=\infty} T_n = T$$

und bezeichnen mit $T_n^{(p)}$ die Summe, die aus T_n entsteht, wenn alle Glieder ausgeschieden werden, in denen x und y beide durch die ungerade Primzahl p teilbar sind, so ergibt sich:

$$T_n^{(p)} = T_n - \frac{1}{p^2}\, T_{n p^{-2}}$$

und durch Grenzübergang zu $n = \infty$:

$$T^{(p)} = T\left(1 - \frac{1}{p^2}\right).$$

Verfährt man so mit allen Primzahlen und setzt

$$S'_{10} + S'_{01} - 2\, S'_{11} = T',$$

so folgt

$$T' = T\, \Pi\left(1 - \frac{1}{p^2}\right),$$

worin sich das Produkt Π auf alle ungeraden Primzahlen p erstreckt. Nun erhält man durch Entwickelung nach steigenden Potenzen von p^{-2}:

$$\frac{1}{\Pi(1 - p^{-2})} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \frac{1}{9^2} + \cdots,$$

$$= \frac{\pi^2}{8},$$

und folglich

$$T = \frac{\pi^2}{8}\, T',$$

und indem man ebenso mit den beiden anderen Summen verfährt, folgt aus (9):

$$\log f(\omega_1) f(\omega_2) = \tfrac{1}{3} \log 2 + \frac{\beta \pi}{24} (S'_{10} + S'_{01} - 2\, S'_{11}),$$

$$(10) \quad \log f_1(\omega_1) f_1(\omega_2) = \tfrac{1}{3} \log 2 + \frac{\beta \pi}{24} (S'_{10} - 2\, S'_{01} + S'_{11}),$$

$$\log f_2(\omega_1) f_2(\omega_2) = \tfrac{1}{3} \log 2 + \frac{\beta \pi}{24} (-2\, S'_{10} + S'_{01} + S'_{11}).$$

Diese Formeln vereinfachen sich wesentlich, wenn man $\alpha = 0$, also

$$\omega_1 = \omega_2 = \omega = i\beta$$

setzt, also wenn man ein rein imaginäres ω annimmt. Dann wird

$$S'_{10} = \Sigma \frac{1}{x^2 - \omega^2 y^2} \qquad \begin{array}{l} x \text{ ungerade, } y \text{ gerade,} \\ xy \text{ relativ prim.} \end{array}$$

Sondert man das Glied $x = \pm 1$, $y = 0$ ab und nimmt von den übrigen je vier zusammen, so ergibt sich

$$S'_{10} = 2 + 4\, \Sigma \frac{1}{x^2 - \omega^2 y^2},$$

worin x, y nur positive Werte durchlaufen.

Ebenso verfährt man mit den anderen Summen. Setzt man dann

$$(11)\qquad \sum \frac{\omega}{y^2\omega^2 - x^2} = S_1 \quad x, y \text{ ungerade,}$$
$$= S_2 \quad x \text{ ungerade, } y \text{ gerade,}$$
$$= S_3 \quad x \text{ gerade, } y \text{ ungerade,}$$

x, y positiv und relativ prim, so folgt:

$$\beta S'_{10} = -2i\omega + 4iS_2,$$
$$\beta S'_{01} = +\frac{2i}{\omega} + 4iS_3,$$
$$\beta S'_{11} = \qquad 4iS_1,$$

und folglich ergibt sich aus (10) für ein rein imaginäres ω:

$$\log f(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(-\omega + \frac{1}{\omega} - 4S_1 + 2S_2 + 2S_3\right),$$
$$(12)\quad \log f_1(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(-\omega - \frac{2}{\omega} + 2S_1 + 2S_2 - 4S_3\right),$$
$$\log f_2(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(2\omega + \frac{1}{\omega} + 2S_1 - 4S_2 + 2S_3\right).$$

§ 148. Elementare Ableitung der Entwickelungen.

Man kann zu den vorstehenden Entwickelungen auch auf dem folgenden Wege gelangen. Es ist nach einer bekannten Formel der Analysis:

$$(1)\qquad \sum_{1,\infty}^{x} \frac{\omega}{\omega^2 y^2 - x^2} = -\frac{1}{2\omega y^2} + \frac{\pi i}{2y}\,\frac{q^{2y}+1}{q^{2y}-1},$$

wenn $q = e^{\pi i \omega}$ ist [1]). Daraus durch Entwickelung nach Potenzen von q:

$$(2)\qquad \sum_{1,\infty}^{x} \frac{\omega}{\omega^2 y^2 - x^2} = -\frac{1}{2\omega y^2} - \frac{\pi i}{y}\left(\frac{1}{2} + \sum_{1,\infty}^{n} q^{2ny}\right).$$

Ersetzt man hier y durch $\frac{1}{2}y$, so folgt:

$$(3)\qquad \sum_{1,\infty}^{x} \frac{2\omega}{\omega^2 y^2 - 4x^2} = -\frac{1}{\omega y^2} - \frac{\pi i}{y}\left(\frac{1}{2} + \sum_{1,\infty} q^{ny}\right),$$

und wenn man (2) von (3) abzieht:

$$(4)\qquad \sum \frac{(-1)^x\omega}{\omega^2 y^2 - x^2} = -\frac{1}{2\omega y^2} - \frac{\pi i}{y}\sum_{1,\infty}^{x} q^{(2n-1)y}.$$

---

[1]) Aus der Entwickelung:
$$\operatorname{cotg} z = \frac{1}{z} + \frac{2z}{z^2-\pi^2} + \frac{2z}{z^2-4\pi^2} + \frac{2z}{z^2-9\pi^2} + \cdots$$

Summiert man diese Formeln abermals nach y von 1 bis ∞ und macht von den Formeln Gebrauch, die teils bekannt sind, teils aus § 24, (11) folgen:

$$\overset{y}{\Sigma}\frac{1}{y^2} = \frac{\pi^2}{6}, \quad \overset{y}{\Sigma}\frac{(-1)^y}{y^2} = -\frac{\pi^2}{12}, \quad \Sigma\frac{(-1)^y}{y} = -\log 2,$$

$$\overset{n}{\Sigma}\overset{y}{\Sigma}\frac{q^{(2n-1)y}}{y} = -\log \Pi(1-q^{2n-1}) = -\log f_1(\omega) - \frac{\pi i \omega}{24},$$

$$\overset{n}{\Sigma}\overset{y}{\Sigma}\frac{(-1)^y q^{2ny}}{y} = -\log \Pi(1+q^{2n}) = -\log f_2(\omega) + \frac{\pi i \omega}{12} - \tfrac{1}{2}\log 2,$$

$$\overset{n}{\Sigma}\overset{y}{\Sigma}\frac{(-1)^y q^{(2n-1)y}}{y} = -\log \Pi(1+q^{2n-1}) = -\log f(\omega) - \frac{\pi i \omega}{24},$$

so ergibt sich:

$$\begin{aligned} \underset{1,\infty}{\overset{y}{\Sigma}}\ \underset{1,\infty}{\overset{x}{\Sigma}}\frac{(-1)^{x+y}\omega}{\omega^2 y^2 - x^2} &= \frac{\pi^2}{24\,\omega} - \frac{\pi^2\omega}{24} + \pi i \log f(\omega), \\ \overset{y}{\Sigma}\ \overset{x}{\Sigma}\frac{(-1)^x\omega}{\omega^2 y^2 - x^2} &= -\frac{\pi^2}{12\,\omega} - \frac{\pi^2\omega}{24} + \pi i \log f_1(\omega), \qquad (5) \\ \overset{y}{\Sigma}\ \overset{x}{\Sigma}\frac{(-1)^y\omega}{\omega^2 y^2 - x^2} &= \frac{\pi^2}{24\,\omega} + \frac{\pi^2\omega}{12} + \pi i \log f_2(\omega). \end{aligned}$$

Die Doppelsummen auf der linken Seite dieser Formeln sind so zu verstehen, daß zuerst die Summation in bezug auf x, dann die Summation in bezug auf y auszuführen ist. Man kann aber auch so summieren, daß man

$$(6) \qquad 0 < x < m, \quad 0 < y < n, \quad n = \infty, \quad \frac{m}{n} = \infty$$

nimmt, und dann m und n so ins Unendliche wachsen läßt, daß $m:n$ unendlich wird. Daß beides dasselbe gibt, kann man auf verschiedene Weise zeigen, z. B. durch Vergleichung der Summen mit Integralen.

Setzt man also, wie in § 147, (10), indem man x, y an die Bedingung (6) bindet:

$$\begin{aligned} \overset{x,y}{\Sigma}\frac{\omega}{\omega^2 y^2 - x^2} &= S_0 \quad x, y \text{ gerade}, \\ &= S_1 \quad x, y \text{ ungerade}, \\ &= S_2 \quad x \text{ ungerade}, y \text{ gerade}, \\ &= S_3 \quad x \text{ gerade}, y \text{ ungerade}, \end{aligned}$$

so folgt aus (5):

$$S_0 + S_1 - S_2 - S_3 = \frac{\pi^2}{24\,\omega} - \frac{\pi^2\omega}{24} + \pi i \log f(\omega),$$
$$S_0 - S_1 - S_2 + S_3 = -\frac{\pi^2}{12\,\omega} - \frac{\pi^2\omega}{24} + \pi i \log f_1(\omega),$$
$$S_0 - S_1 + S_2 - S_3 = \frac{\pi^2}{24\,\omega} + \frac{\pi^2\omega}{12} + \pi i \log f_2(\omega).$$

Daraus durch Addition:

$$3\,S_0 - S_1 - S_2 - S_3 = \pi i \log \sqrt{2},$$

und wenn man S_0 eliminiert:

$$\tfrac{4}{3}S_1 - \tfrac{2}{3}S_2 - \tfrac{2}{3}S_3 = \frac{\pi^2}{24\,\omega} - \frac{\pi^2\omega}{24} - \frac{\pi i}{3}\log\sqrt{2} + \pi i \log f(\omega),$$
$$-\tfrac{2}{3}S_1 - \tfrac{2}{3}S_2 + \tfrac{4}{3}S_3 = -\frac{\pi^2}{12\,\omega} - \frac{\pi^2\omega}{24} - \frac{\pi i}{3}\log\sqrt{2} + \pi i \log f_1(\omega),$$
$$-\tfrac{2}{3}S_1 + \tfrac{4}{3}S_2 - \tfrac{2}{3}S_3 = \frac{\pi^2}{24\,\omega} + \frac{\pi^2\omega}{12} - \frac{\pi i}{3}\log\sqrt{2} + \pi i \log f_2(\omega).$$

Man kann nun ebenso wie vorhin von den Summen S zu den S' übergehen, in denen x, y relativ prim sind, und findet:

$$\log f(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(-\omega + \frac{1}{\omega} - 4\,S_1' + 2\,S_2' + 2\,S_3'\right),$$
$$(7)\qquad \log f_1(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(-\omega - \frac{2}{\omega} + 2\,S_1' + 2\,S_2' - 4\,S_3'\right),$$
$$\log f_2(\omega) = \tfrac{1}{3}\log\sqrt{2} + \frac{\pi i}{24}\left(-\omega - \frac{1}{\omega} + 2\,S_1' - 4\,S_2' + 2\,S_3'\right).$$

Diese Formeln stimmen der Form nach mit § 147, (11) überein, was insofern auffallend ist, als die Art des Grenzüberganges beide Male eine verschiedene ist.

§ 149. Entwickelungen für die Funktion $\log \eta(\omega)$.

Betrachten wir die Summe

$$(1)\qquad U = \sum^{x,y} \frac{1}{(x+\omega y)^{2s}},$$

erstreckt über alle x, y mit Ausnahme der Kombination 0, 0.

Indem man die Glieder mit $y = 0$ absondert, kann man dafür setzen:

$$(2)\qquad U = 2\sum_{1,\infty}^{x} \frac{1}{x^{2s}} + 2\sum_{1,\infty}^{y}\ \sum_{-\infty,\infty}^{x} \frac{1}{(x+\omega y)^{2s}};$$

sodann ist

$$\frac{\Gamma(2s)}{[-2\pi i(x+\omega y)]^{2s}} = \int_0^\infty e^{2\pi i(x+y\omega)\xi}\,\xi^{2s-1}\,d\xi,$$

$$= \int_0^1 e^{2\pi i x\xi} \sum_{0,\infty}^{n} e^{2\pi i y\omega(\xi+n)}\,(\xi+n)^{2s-1}\,d\xi.$$

Summiert man nun nach x und wendet die Fouriersche Reihe an:

$$\sum^{x}\int_0^1 e^{2\pi i x\xi} f(\xi)\,d\xi = \tfrac{1}{2}[f(0)+f(1)],$$

so folgt:

$$\frac{\Gamma(2s)}{(-2\pi i)^{2s}} \sum_{-\infty,\infty}^{x} \frac{1}{(x+\omega y)^{2s}} = \sum_{1,\infty}^{n} e^{2\pi i y\omega n}\, n^{2s-1},$$

und durch Summation nach y:

$$\frac{\Gamma(2s)}{(-2\pi i)^{2s}} \sum_{1,\infty}^{y} \sum_{-\infty,\infty}^{x} \frac{1}{(x+\omega y)^{2s}} = \sum_{1,\infty}^{n} \frac{e^{2\pi i\omega n}}{1-e^{2\pi i\omega n}}\, n^{2s-1}$$

$$= -\frac{1}{2\pi i}\sum_{1,\infty}^{n} \frac{d\log(1-e^{2\pi i\omega n})}{d\omega}\, n^{2s-2}.$$

Hiernach bekommen wir durch den Grenzübergang mit Rücksicht auf die Definition der Funktion $\eta(\omega)$ [§ 24, (8)]:

$$\operatorname*{Lim}_{s=1} \sum_{1,\infty}^{y} \sum^{x} \frac{1}{(x+\omega y)^{2s}} = -2\pi i\,\frac{d\log\eta(\omega)}{d\omega} - \frac{\pi^2}{6}.$$

Ferner ist

$$\operatorname{Lim} \sum \frac{1}{x^{2s}} = \frac{\pi^2}{6},$$

und demnach folgt (1) und (2):

$$(3) \qquad \operatorname*{Lim}_{s=1} \sum^{x,y} \frac{1}{(x+\omega y)^{2s}} = -4\pi i\,\frac{d\log\eta(\omega)}{d\omega}$$

[zu summieren, wie zu (1) angegeben]. Wollte man hier unter dem Summenzeichen zur Grenze übergehen, so würde man erhalten:

$$(4) \qquad -4\pi i\,\frac{d\log\eta(\omega)}{d\omega} = \sum^{x,y} \frac{1}{(x+\omega y)^2},$$

dann aber würde man eine nur bedingt konvergente Summe haben, und es müßte eine genaue Art des Grenzüberganges festgestellt werden. Man müßte in der xy-Ebene eine geschlossene Kurve annehmen, innerhalb deren die Punkte x, y liegen, und dann diese Kurve ins Unendliche hinausrücken lassen. Der Wert der Summe wird von der Beschaffenheit dieser Kurve abhängen. Vielleicht ergibt sich dafür die Ellipse $|x+\omega y| = n$. An sich hat die Formel (4) keinen Sinn.

VIERTES BUCH.

KLASSENKÖRPER.





Dreiundzwanzigster Abschnitt.

Der Teilungskörper.

§ 150. Die homogenen Weierstrassschen Funktionen.

Wir waren in § 114 von der Frage ausgegangen, unter welchen Voraussetzungen eine doppelt periodische Funktion $\varphi(u)$ mit den Perioden ω_1, ω_2 eine Multiplikation $\varphi(\mu u)$ gestattet, d. h. unter welchen Umständen $\mu\omega_1$, $\mu\omega_2$ sich linear und ganzzahlig durch ω_1, ω_2 ausdrücken lassen, und waren zu dem Resultat gelangt, daß dies bei veränderlichem ω_1, ω_2 nur möglich ist, wenn μ eine ganze rationale Zahl ist, und daß nur, wenn

$$\omega = \frac{\omega_2}{\omega_1} \tag{1}$$

eine imaginäre quadratische Irrationalzahl ist, auch μ eine komplexe Zahl desselben Körpers wie ω sein kann. Es kommt jetzt darauf an, die aus dieser Annahme folgenden Formeln der komplexen Multiplikation etwas genauer zu erforschen.

Wir wollen zunächst, als das formal einfachere, die komplexe Multiplikation der Weierstrassschen elliptischen Funktion $\wp(u)$ untersuchen, müssen dann aber auch noch die komplexe Multiplikation der Jacobischen elliptischen Funktionen in Betracht ziehen.

In den § 37, (8), § 46, (13) haben wir die Formeln für die Homogeneität der Funktionen $\sigma(u)$, $\wp(u)$ und der Invarianten g_2, g_3, $16\,G = g_2^3 - 27\,g_3^2$ abgeleitet, die wir hier noch einmal zusammenstellen:

$$\begin{aligned}
\sigma(\lambda u, \lambda\omega_1, \lambda\omega_2) &= \lambda\ \ \sigma(u, \omega_1, \omega_2),\\
\wp(\lambda u, \lambda\omega_1, \lambda\omega_2) &= \lambda^{-2}\,\wp(u, \omega_1, \omega_2),\\
g_2(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-4}\,g_2(\omega_1, \omega_2),\\
g_3(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-6}\,g_3(\omega_1, \omega_2),\\
G(\lambda\omega_1, \lambda\omega_2) &= \lambda^{-12}\,G(\omega_1, \omega_2),
\end{aligned} \tag{2}$$

und die Funktionen § 46, (12), (15), (16):

$$(3)\qquad \frac{4.27\, g_2^3}{G} = j(\omega),$$

$$\frac{4.27.27\, g_3^2}{G} = j(\omega) - 27.64,$$

$$\omega_1^{12}\, G = 2^8 \pi^{12} \eta(\omega)^{24}$$

hängen von dem Verhältnis (1) ab.

In § 54, (4), (5) sind noch die eindeutigen Funktionen von ω:

$$(4)\qquad \gamma_2(\omega) = \sqrt[3]{j(\omega)} = \frac{f(\omega)^{24} - 16}{f(\omega)^8},$$

$$\gamma_3(\omega) = \sqrt{j(\omega) - 27.64} = \frac{[f(\omega)^{24} + 8]\,[f_1(\omega)^8 - f_2(\omega)^8]}{f(\omega)^8}$$

definiert.

Aus der letzten Gleichung (3) erkennt man [etwa aus der Entwickelung von $\eta(\omega)$, § 24, (8)], daß G nicht verschwinden kann, solange ω einen positiv imaginären Bestandteil hat, und folglich können auch g_2, g_3 nicht beide zugleich verschwinden.

Aus den Reihenentwickelungen des § 56 ergibt sich:

$$(5)\qquad \sigma(u) = \sum^{m,n} a_{m,n} (\tfrac{1}{2} g_2)^m (2 g_3)^n \frac{u^{2\nu+1}}{(2\nu+1)!},$$

$$\nu = 2m + 3n,$$

worin die rationalen Koeffizienten $a_{m,n}$ nur Potenzen von 3 im Nenner haben können (nach Schwarz-Weierstrass sind es ganze Zahlen, worauf es hier aber nicht ankommt).

Ebenso ist

$$(6)\qquad \wp(u) = \Sigma\, b_{m,n} (\tfrac{1}{2} g_2)^m (2 g_3)^n \frac{u^{2\nu-2}}{(2\nu+1)!}$$

mit rationalen Koeffizienten $b_{m,n}$. Um Funktionen von zwei Variablen zu erhalten, machen wir folgende Substitution:

Wenn von den beiden Invarianten g_2, g_3 keine verschwindet, so setzen wir:

$$(7)\qquad u = \sqrt{\frac{g_2 g_3}{G}}\, w,$$

also

$$g_2^m g_3^n u^{2\nu+1} = \left(\frac{g_2^3}{G}\right)^{m+n} \left(\frac{g_2^2}{G}\right)^{m+2n} \sqrt{\frac{g_2 g_3}{G}}\, w^{2\nu+1},$$

und dadurch ergibt sich aus (5):

$$(8)\qquad \sqrt{\frac{G}{g_2 g_3}}\, \sigma(u) = \Sigma\, A_{m,n}\, j^{m+n} (j - 27.64)^{m+2n} \frac{w^{2\nu+1}}{(2\nu+1)!}$$

worin die $A_{m,n}$ rationale Zahlen sind, die im Nenner nur Potenzen von 2 und von 3 enthalten können

In gleicher Weise ergibt sich aus der Reihenentwickelung (6) für die $\wp$-Funktion:

$$(9)\quad \frac{g_2 g_3}{G} \wp(u) = \sum^{m,n} B_{m,n} j^{m+n} (j - 27 . 64)^{m+2n} \frac{w^{2\nu-2}}{(2\nu+1)!},$$

worin die $B_{m,n}$ rationale Zahlkoeffizienten sind. Daß auch sie nur Potenzen von 2 und 3 im Nenner haben, machen die ersten Fälle wahrscheinlich, kommt aber für uns jetzt nicht in Betracht.

Ist g_2 oder g_3 gleich Null, so ist die Substitution (7) nicht brauchbar. Ist zunächst

$$g_3 = 0,$$

so fallen in den Reihen für $\sigma(u)$ und $\wp(u)$ die Glieder weg, in denen n positiv ist. Es ist dann

$$\sigma(u) = \Sigma\, a_{m,0}\, g_2^m \frac{u^{4m+1}}{(4m+1)!},$$

$$\wp(u) = \Sigma\, b_{m,0}\, g_2^m \frac{u^{4m-2}}{(2m+1)!}.$$

Wir setzen dann

$$(10)\quad u = g_2^{-\frac{1}{4}} w$$

und erhalten

$$(11)\quad \begin{aligned} g_2^{\frac{1}{4}} \sigma(u) &= \sum^{m} A_m \frac{w^{4m+1}}{(4m+1)!}, \\ g_2^{-\frac{1}{2}} \wp(u) &= \sum^{m} B_m \frac{w^{4m-2}}{(4m+1)!}, \end{aligned}$$

wenn A_m, B_m wieder rationale Zahlen sind.

Ist endlich

$$g_2 = 0,$$

so setzen wir

$$(12)\quad u = g_3^{-\frac{1}{6}} w,$$

und erhalten

$$(13)\quad \begin{aligned} g_3^{\frac{1}{6}} \sigma(u) &= \sum^{n} A_n \frac{w^{6n+1}}{(6n+1)!}, \\ g_3^{-\frac{1}{3}} \wp(u) &= \sum^{n} B_n \frac{w^{6n-2}}{(6n+1)!}. \end{aligned}$$

In den Entwickelungen (8), (9), (11), (13) ist

$$(14)\quad A_{00} = 1, \quad B_{00} = 1, \quad A_0 = 1, \quad B_0 = 1.$$

§ 151. Die komplexe Multiplikation der Funktion $\wp(u)$.

Wir nehmen jetzt an, die Perioden ω_1, ω_2 der Funktion $\wp(u)$ genügen einer quadratischen Gleichung

$$(1) \qquad A\omega_2^2 + B\omega_2\omega_1 + C\omega_1^2 = 0,$$

in der A, B, C ganze rationale Zahlen ohne gemeinschaftlichen Teiler sind. Es sei A positiv, und die Diskriminante der quadratischen Form (A, B, C)

$$(2) \qquad B^2 - 4AC = \Delta$$

sei eine negative Stammdiskriminante, d. h. es enthalte Δ keinen quadratischen Faktor, nach dessen Absonderung eine Diskriminante übrig bleibt (§ 84).

Setzen wir

$$(3) \qquad \omega = \frac{\omega_2}{\omega_1},$$

so folgt aus (1):

$$(4) \qquad 2A\omega = -B + \sqrt{\Delta},$$

und wenn wir $\sqrt{\Delta}$ positiv imaginär annehmen, so erhält ω einen positiv imaginären Teil und kann als Modul einer ϑ-Funktion dienen. Δ ist die Grundzahl eines imaginären quadratischen Körpers, den wir mit Ω bezeichnen [1].

Durch die singuläre Invariante $j(\omega)$ wird der Klassenkörper $\mathfrak{K}(\Delta)$ bestimmt, dessen Relativgrad in bezug auf Ω gleich der Klassenzahl der Diskriminante Δ ist. Die ganzen Zahlen des quadratischen Körpers $\Omega = \Re(\sqrt{\Delta})$ sind von der Form:

$$(5) \qquad \mu = \frac{x + y\sqrt{\Delta}}{2},$$

worin x und y ganze rationale Zahlen sind, die der Bedingung

$$x \equiv By \pmod 2$$

genügen. Zu der durch (5) definierten Zahl μ bestimmen wir vier ganze rationale Zahlen a, b, c, ∂:

$$(6) \qquad \begin{aligned} a &= \frac{x + By}{2}, & b &= Ay, \\ c &= -Cy, & \partial &= \frac{x - By}{2}, \end{aligned}$$

---

[1] Die Annahme, daß Δ Stammdiskriminante sei, ist hier zur Vereinfachung gemacht. In meiner Abhandlung „Über Zahlgruppen in algebraischen Körpern" (Mathematische Annalen, Bd. L) ist diese Annahme nicht gemacht. Man erhält dann allgemeinere Körper, die zu den Ordnungen gehören, wie in § 124.

woraus:

$$(7) \qquad a\partial - bc = \frac{x^2 - \Delta y^2}{4} = \mu\mu' = m,$$

wenn

$$(8) \qquad \mu' = \frac{x - y\sqrt{\Delta}}{2}$$

die zu μ konjugierte Zahl des Körpers Ω ist.

Nehmen wir y von Null verschieden, so folgt aus (1) durch Multiplikation mit y:

$$b\,\omega_2^2 + (a - \partial)\,\omega_2\,\omega_1 - c\,\omega_1^2 = 0,$$

und dafür kann man auch schreiben:

$$(a\,\omega_1 + b\,\omega_2)\,\omega_2 = (c\,\omega_1 + \partial\,\omega_2)\,\omega_1$$

oder

$$(9) \qquad \omega = \frac{c + \partial\,\omega}{a + b\,\omega}.$$

Nach (4) und (5) folgt aus (6):

$$(10) \qquad a + b\,\omega = \frac{x + (2A\,\omega + B)\,y}{2} = \mu,$$
$$c + \partial\,\omega = \mu\,\omega,$$

oder in homogener Form:

$$(11) \qquad \begin{aligned} \mu\,\omega_1 &= a\,\omega_1 + b\,\omega_2, \\ \mu\,\omega_2 &= c\,\omega_1 + \partial\,\omega_2, \end{aligned}$$

und durch Auflösung dieser linearen Gleichungen:

$$(12) \qquad \begin{aligned} \mu'\,\omega_1 &= \partial\,\omega_1 - b\,\omega_2, \\ \mu'\,\omega_2 &= -c\,\omega_1 + a\,\omega_2. \end{aligned}$$

Daraus ergibt sich, daß $\wp(\mu u)$ eine doppelt-periodische Funktion mit den Perioden ω_1, ω_2 ist, und da sie außerdem eine gerade Funktion von u ist, so läßt sie sich rational durch $\wp(u)$ darstellen (§ 21). Wenn wir also mit R und P ganze rationale Funktionen von $\wp(u)$ ohne gemeinschaftlichen Teiler bezeichnen, so ist

$$(13) \qquad \wp(\mu u) = \frac{R}{P}.$$

Da der Quotient $\wp(\mu u) : \wp(u)$ für $u = 0$, d. h. für $\wp(u) = \infty$, endlich bleibt, so ist der Grad von R um eine Einheit höher als der Grad des Nenners.

§ 152. Die Pole der Funktion $\wp(\mu u)$.

Um den Grad der Funktionen R und P festzustellen, müssen wir die Nullstellen von P, also die Unendlichkeitsstellen von $\wp(\mu u)$, abzählen, die nicht zugleich Unendlichkeitsstellen von $\wp(u)$ sind. Es wird aber $\wp(\mu u):\wp(u)$ dann und nur dann unendlich, wenn

(1) $$u = \frac{h_1 \omega_1 + h_2 \omega_2}{\mu}$$

wird, wenn h_1, h_2 ganze Zahlen sind, wenn $h_1 \omega_1 + h_2 \omega_2$, aber nicht $(h_1 \omega_1 + h_2 \omega_2):\mu$ eine Periode ist. Setzen wir also

(2) $$\wp(\mu u) = \frac{R_\mu[\wp(u)]}{P_\mu[\wp(u)]},$$

und bezeichnen mit g die Wurzeln von $P_\mu(x)$, so ist

(3) $$g = \wp\left(\frac{h_1 \omega_1 + h_2 \omega_2}{\mu}\right).$$

Die Zahl g ändert sich nicht, wenn h_1 und h_2 um Vielfache von $m = \mu\mu'$ geändert werden, weil dadurch nach (11), § 151 das Argument der $\wp$-Funktionen um eine Periode geändert wird.

Da die Funktionen $\wp(u)$ und $\wp(\mu u)$ nicht geändert werden, wenn wir die Periode ω_1, ω_2 einer linearen Transformation mit der Determinante 1 unterwerfen, so beschränken wir die Allgemeinheit nicht, wenn wir annehmen, A sei relativ prim zu m und wegen der Periodizität von $\wp(u)$ können wir daher auch setzen:

$$g = \wp\left(\frac{h_1 \omega_1 + h_2 A \omega_2}{\mu}\right).$$

Wegen der Homogenität von $\wp(u)$ können wir nun $\omega_1 = 1$, $\omega_2 = \omega$ setzen und erhalten nach § 151, (4):

$$A\omega = \frac{-B + \sqrt{\Delta}}{2},$$

und demnach ist

(4) $$h_1 \omega_1 + h_2 A \omega_2 = h_1 + h_2\left(\frac{-B + \sqrt{\Delta}}{2}\right).$$

Wenn wir daher

$$h_1 + h_2 \frac{-B + \sqrt{\Delta}}{2} = v$$

setzen, so ergibt sich aus (3):

(5) $$g = \wp\left(\frac{v}{\mu}\right),$$

worin ν ebenso wie μ eine ganze Zahl des Körpers Ω ist, die nicht durch μ teilbar ist.

Ist diese Bedingung erfüllt, so ist g eine Wurzel von $P_\mu(x)$. Weil aber $\wp(\mu u)$ in der u-Ebene für $u \equiv 0$ (modd. ω_1, ω_2) unendlich in der zweiten Ordnung wird, so ist $P_\mu(x)$ durch $(x-g)^2$ teilbar, es sei denn, daß

$$\wp(u) - g$$

für $u = \nu : \mu$ selbst in der zweiten Ordnung verschwindet; dies tritt wegen § 46, (18) dann ein, wenn

$$\wp'\left(\frac{\nu}{\mu}\right) = 0$$

ist, also wenn $\nu : \mu$ eine halbe Periode ist, und also

(6) $$g = e_1,\ e_2,\ e_3$$

wird.

1. Nach (4) ist, wenn $\omega_1 = 1$, $\omega_2 = \omega$ gesetzt ist, jede ganze Zahl des Körpers Ω eine Periode von $\wp(u)$. Dies gilt nicht umgekehrt; da aber $A\omega$ eine ganze Zahl in Ω ist, so muß jede Periode durch Multiplikation mit A in eine ganze Zahl verwandelt werden.

Daraus folgt, daß zwei Werte

$$g = \wp\left(\frac{\nu}{\mu}\right), \quad g' = \wp\left(\frac{\nu'}{\mu}\right)$$

dann und nur dann einander gleich sind, wenn

$$\nu \equiv \pm \nu' \pmod{\mu}$$

ist. Denn ist $g = g'$, so muß entweder

$$\frac{\nu + \nu'}{\mu} \quad \text{oder} \quad \frac{\nu - \nu'}{\mu}$$

durch Multiplikation mit A in eine ganze Zahl verwandelt werden. A ist aber relativ prim zu μ, und folglich muß eine dieser beiden Zahlen selbst ganz sein. Die Anzahl der inkongruenten Werte von ν ist aber gleich $N(\mu) = m$ (Bd. II, § 165).

Lassen wir also ν ein volles Restsystem nach dem Modul μ mit Ausschluß der Null durchlaufen, so bekommen wir jeden Wert von g zweimal, außer wenn

(7) $$2\nu \equiv 0 \pmod{\mu},$$

und in diesem Falle ist $\wp\left(\frac{\nu}{\mu}\right)$ einer der Werte e. Daraus folgt:

(8) $$P_\mu(x) = \Pi\left[x - \wp\left(\frac{\nu}{\mu}\right)\right],$$

und $P_\mu(x)$ ist vom Grade $m - 1$.

In dem Produkt $P_\mu(x)$ kommt jeder Faktor $x - g$ zweimal vor, außer wenn g einem der e gleich ist, wenn also die Kongruenz (7) für ein von Null verschiedenes ν erfüllt werden kann.

1) Wenn μ relativ prim zu 2 ist, also wenn m ungerade ist, so hat die Kongruenz (7) nur die Wurzel $\nu = 0$. Dann ist $P_\mu(x)$ ein Quadrat, und wenn $S(x)$ eine Funktion vom Grade $\frac{1}{2}(m - 1)$ ist,

(9) $$P_\mu(x) = S^2, \quad m \equiv 1 \pmod 2.$$

Wenn μ mit 2 einen Teiler gemein hat, sind drei Fälle zu unterscheiden.

2) Wenn μ durch 2 teilbar ist, so muß ν, wenn es der Kongruenz (7) genügen soll, ein Vielfaches von $\frac{1}{2}\mu$ sein, und da es drei von Null verschiedene nach dem Modul 2 inkongruente Zahlen in Ω gibt, so hat (7) drei Wurzeln. Es kommen also unter den g die drei Werte e_1, e_2, e_3 vor, und wir haben:

(10) $$P_\mu(x) = \wp'(u)^2 S^2, \quad m \equiv 0 \pmod 2,$$

worin S eine ganze Funktion vom Grade $\frac{1}{2}m - 2$ ist.

3) Wenn 2 im Körper Ω in zwei (gleiche oder verschiedene) Primideale zerfällt, also wenn $\Delta \equiv 0 \pmod 4$ oder $\equiv 1 \pmod 8$ ist, so kann μ durch einen dieser Primfaktoren teilbar sein, ohne durch 2 teilbar zu sein. Dann hat die Kongruenz (7) nur eine von Null verschiedene Wurzel und es kommt unter den Zahlen g nur eine der drei Zahlen (6), etwa e, vor. In diesem Falle ist

(11) $$P_\mu(x) = [\wp(u) - e]\, S^2,$$

worin S eine Funktion vom Grade $\frac{1}{2}m - 1$ ist.

In bezug auf die beiden besonderen Fälle $g_3 = 0$ und $g_2 = 0$ ist noch folgendes zu bemerken.

4) Wenn $g_3 = 0$ ist, so ist $\Delta = -4$, $j(\omega) = 0$, und es ergibt sich aus der Differentialgleichung § 46, (18):

$$\wp'(u)^2 = 4\wp(u)^3 - g_2\wp(u),$$

durch die mit Rücksicht auf das Anfangsglied der Entwickelung die $\wp$-Funktion eindeutig bestimmt ist.

Ersetzt man dann u durch iu, so folgt:

$$-[\wp'(iu)]^2 = 4\wp^3(iu) - g_2\wp(iu),$$

und daraus:

$$(12)\qquad \wp(iu) = -\wp(u).$$

Die Größen g sind also einander paarweise entgegengesetzt, eine der drei Größen e_1, e_2, e_3 ist gleich Null, die beiden anderen ebenfalls entgegengesetzt gleich. Daraus folgt, daß in den Formeln (9) bis (11) die Funktion S in diesem Falle nur die geraden Potenzen von $\wp(u)$ enthalten kann.

5) Ist $g_2 = 0$, so ist $\varDelta = -3$, $j(\omega) = 64.27$, und es ist, wenn mit ϱ eine imaginäre dritte Einheitswurzel bezeichnet wird:

$$(13)\qquad \wp(u) = \varrho\,\wp(\varrho^2 u) = \varrho^2\,\wp(\varrho u),$$

und die Wurzeln g von S ordnen sich zu dreien in der Weise:

$$(14)\qquad g,\quad \varrho g,\quad \varrho^2 g.$$

Unter diesen drei Werten sind nur dann zwei einander gleich, wenn sie alle drei verschwinden. Aus (13) aber ergibt sich, daß dies eintritt, wenn u mit einem der Werte $\pm 1 : \sqrt{-3}$ kongruent wird. Denn für $\varDelta = -3$ sind $1, \varrho, \varrho^2$ Perioden von $\wp(u)$, und da nun

$$\frac{\varrho - \varrho^2}{\sqrt{-3}} = 1$$

ist, so ist nach (13):

$$\wp\left(\frac{\varrho}{\sqrt{-3}}\right) = \wp\left(\frac{\varrho^2}{\sqrt{-3}}\right) = 0,$$

und der Wert Null kommt also unter den g dann und nur dann vor, wenn m durch 3 teilbar ist.

Daraus folgt:

Ist $\varDelta = -3$ und $m \equiv 0 \pmod 3$, so ist $S : \wp(u)$ eine rationale Funktion von $\wp(u)^3$.

Ist $\varDelta = -3$ und $m \equiv 1 \pmod 3$, so ist S selbst eine rationale Funktion von $\wp(u)^3$.

[Da m die Form $\frac{1}{4}(x^2 + 3y^2)$ haben muß, so kann hier m nicht $\equiv -1 \pmod 3$ sein.]

§ 153. Die Funktion $\tau(u)$.

Wir führen nun nach § 150 (6), (8), (9), (10), (12), (13) eine Funktion $\tau = \tau(u)$ ein, die nur von zwei Argumenten w, ω abhängt, indem wir setzen:

$$(1) \qquad \begin{aligned} &\text{a)} \quad \tau(u) = \frac{g_2 g_3}{G} \wp(u), && \text{im allgemeinen,} \\ &\text{b)} \quad = \frac{\wp(u)^2}{g_2}, && \text{wenn } g_3 = 0, \\ &\text{c)} \quad = \frac{\wp(u)^3}{g_3}, && \text{wenn } g_2 = 0. \end{aligned}$$

Und wenn dann μ wie oben eine ganze Zahl des Körpers Ω ist, so können wir in allen drei Fällen setzen:

$$(2) \qquad \tau(\mu u) = \frac{\Psi(\tau)}{\Phi(\tau)},$$

worin Φ, Ψ ganze Funktionen von τ sind, die bis auf konstante Faktoren im Falle (1) a) mit R, P des vorigen Paragraphen übereinstimmen, in den Fällen (1) b) und (1) c) daraus durch Erhebung ins Quadrat oder in den Kubus hervorgehen [§ 152, 4), 5)].

Wir richten den Bruch (2) so ein, daß die höchste Potenz von τ im Nenner Φ den Koeffizienten 1 hat. Die übrigen Koeffizienten von Φ sind dann rational zusammengesetzt aus Größen der Form

$$\tau\left(\frac{\nu}{\mu}\right) = \tau\left(\frac{\nu\mu'}{m}\right),$$

und da $\nu\mu'$ eine Periode von τ ist, so gehören diese Größen zu den Wurzeln der Teilungsgleichung der Perioden, und sind daher, da der Modul der entsprechenden elliptischen Funktionen eine algebraische Zahl ist, selbst algebraische Zahlen (§ 58, § 61).

Daraus folgt:

2. Die Koeffizienten in $\Phi(\tau)$ sind algebraische Zahlen.

Wir erweitern den Bruch $\Psi : \Phi$ durch Multiplikation von Zähler und Nenner mit dem Produkt der konjugierten Werte Φ', Φ'', Φ''', ... und erhalten:

$$(3) \qquad \tau(\mu u) = \frac{Z}{N},$$

worin nun Z und N ganze Funktionen von τ sind, die einen gemeinsamen Teiler enthalten können, wobei jedoch N rationale Zahlenkoeffizienten hat.

Nach § 150, (8), (10), (13) beginnt die Entwickelung von $\tau(u)$ nach steigenden Potenzen von u mit einer negativen Potenz von u. Wir ordnen in der Gleichung

$$\tau(\mu u) N = Z \tag{4}$$

die Funktion Z nach fallenden Potenzen von τ, entwickeln beide Seiten nach steigenden Potenzen von u und vergleichen die Koeffizienten gleich hoher Potenzen von u. Dann bekommen wir für die Bestimmung der Koeffizienten von Z eine Reihe linearer Gleichungen, deren jede folgende nur einen neuen dieser Koeffizienten enthält, und daraus können diese Koeffizienten successive rational berechnet werden. Beachtet man nun die Form der Entwickelungen des § 150, so ergibt sich, daß die Koeffizienten von Z rationale Funktionen von $j(\omega)$ und $\sqrt{\Delta}$ sind.

Befreit man nach dem Euklidischen Algorithmus N und Z von gemeinschaftlichen Faktoren, so kommt man zu den Funktionen Ψ, Φ zurück, und es ergibt sich, wenn wir unter dem Klassenkörper den Inbegriff der rationalen Funktionen von $\sqrt{\Delta}$ und $j(\omega)$ verstehen:

3. Die Koeffizienten der Funktionen $\Phi(\tau)$, $\Psi(\tau)$ in (2) gehören dem Klassenkörper an.

§ 154. Der Teilungskörper.

Wenn wir (durch rationale Rechnung) die Funktion $\Phi(x)$ von allen mehrfach darin vorkommenden Faktoren befreien, so bleibt eine ganze Funktion $T_\mu(x)$ von x übrig, deren Koeffizienten dem Klassenkörper angehören, und die Wurzeln von $T_\mu(x)$ sind sämtliche voneinander verschiedene unter den Größen

$$\tau\left(\frac{\nu}{\mu}\right). \tag{1}$$

Zwei dieser Größen

$$\tau\left(\frac{\nu}{\mu}\right), \quad \tau\left(\frac{\nu'}{\mu}\right)$$

sind einander gleich,

im Falle (1) a), wenn $\dfrac{\nu}{\mu} \equiv \pm\dfrac{\nu'}{\mu}$,

(1) b), wenn $\dfrac{\nu}{\mu} \equiv \pm\dfrac{\nu'}{\mu} \equiv \pm i\dfrac{\nu'}{\mu}$,

(1) c), wenn $\dfrac{\nu}{\mu} \equiv \pm\dfrac{\nu'}{\mu}, \quad \pm\varrho\dfrac{\nu'}{\mu}, \quad \pm\varrho^2\dfrac{\nu'}{\mu}$,

worin die Kongruenz auf die Perioden bezogen wird, also (§ 152, 1.)

$$\text{(2)}\qquad \begin{array}{ll} \text{im Falle a), wenn } \nu \equiv \pm\nu', & \\ \qquad\quad \text{b), wenn } \nu \equiv \pm\nu',\ \pm i\nu' & \pmod{\mu}, \\ \qquad\quad \text{c), wenn } \nu \equiv \pm\nu',\ \pm\varrho\nu',\ \pm\varrho^2\nu'. & \end{array}$$

Es seien jetzt

$$\text{(3)}\qquad \mu = \mathfrak{a}\,\mathfrak{m}, \quad \mu_1 = \mathfrak{a}_1\,\mathfrak{m}$$

zwei ganze Zahlen mit dem größten gemeinschaftlichen Idealteiler $\mathfrak{m}$ im Körper Ω. Dann haben T_μ und T_{μ_1} einen gemeinsamen Linearteiler, wenn

$$\text{(4)}\qquad \tau\left(\frac{\nu}{\mu}\right) = \tau\left(\frac{\nu_1}{\mu_1}\right),$$

und dies findet nach (2) dann und nur dann statt, wenn

$$\text{(5)}\qquad \mu\,\nu_1 \equiv \varepsilon\,\mu_1\,\nu \pmod{\mu\,\mu_1},$$

worin ε eine Einheit des Körpers Ω ist, also $\varepsilon = \pm 1$ im allgemeinen, $\varepsilon = \pm 1, \pm i$, wenn $\Delta = -4$, und $\varepsilon = \pm 1, \pm\varrho, \pm\varrho^2$, wenn $\Delta = -3$ ist. Aus (5) folgt aber, daß ν durch $\mathfrak{a}$ und ν_1 durch $\mathfrak{a}_1$ teilbar sein muß.

Denken wir uns ν gegeben und ν_1 gesucht, so ist die Kongruenz (5) nur möglich, wenn $\mu_1\nu$ durch μ teilbar ist, und da $\mathfrak{a}$ und $\mathfrak{a}_1$ relativ prim sind, so muß ν durch $\mathfrak{a}$ teilbar sein. Ist α eine durch $\mathfrak{a}$ teilbare ganze Zahl in Ω, so beschaffen, daß $\alpha:\mathfrak{a}$ relativ prim zu $\mathfrak{m}$ ist, so können wir demnach

$$\text{(6)}\qquad \nu \equiv \alpha\,\xi \pmod{\mu}$$

setzen (Bd. II, § 166, 7.) und erhalten die sämtlichen voneinander verschiedenen Werte $\tau\left(\frac{\nu}{\mu}\right)$, und jeden zwei-, vier- oder sechsmal, wenn wir ξ ein volles Restsystem nach dem Modul $\mathfrak{m}$ durchlaufen lassen (mit Ausschluß der Null). Man erhält dann die sämtlichen gemeinsamen Wurzeln von T_μ und T_{μ_1} in der Form

$$\text{(7)}\qquad \tau_\xi = \tau\left(\frac{\alpha\,\xi}{\mu}\right).$$

Der größte gemeinschaftliche Teiler $D_\mathfrak{m}$ von T_μ und T_{μ_1} hat also alle die Größen (7) zu Wurzeln. Aus $D_\mathfrak{m}$ läßt sich noch auf rationalem Wege ein Teiler $T_\mathfrak{m}$ absondern, der nur die unter den Größen (7) zu Wurzeln hat, in denen ξ relativ prim zu $\mathfrak{m}$ ist, wenn man $D_\mathfrak{m}$ von allen Faktoren befreit, die es mit einem $D_{\mathfrak{m}'}$ gemein hat, wenn $\mathfrak{m}'$ ein Teiler von $\mathfrak{m}$ ist. Da in dieser

Betrachtung in (3) $\mathfrak{m}$ jedes beliebige Ideal in Ω bedeuten kann, so kommen wir zu folgendem **Hauptsatz**:

4. **Ist $\mathfrak{m}$ ein beliebiges Ideal des Körpers Ω, so existiert eine Funktion $T_\mathfrak{m}$ in Ω, deren Wurzeln die voneinander verschiedenen der Zahlen τ_ξ sind, wenn ξ ein System inkongruenter, zu $\mathfrak{m}$ teilerfremder Zahlen durchläuft.**

Um den Grad der Funktion $T_\mathfrak{m}$ zu bestimmen, bemerken wir, daß zwei Größen τ_ξ, $\tau_{\xi'}$ nur dann einander gleich sind, wenn

(8) $$\xi \equiv \varepsilon\, \xi' \pmod{\mathfrak{m}}$$

ist. Es werden also so viele von den τ_ξ einander gleich, als es modulo $\mathfrak{m}$ inkongruente Einheiten gibt; das sind im allgemeinen zwei, für $\Delta = -4$ sind es vier und für $\Delta = -3$ sind es sechs. Diese Zahlen verringern sich aber wiederum, wenn verschiedene der Einheiten ε nach dem Modul $\mathfrak{m}$ kongruent sind, wenn also $1 - \varepsilon$ durch $\mathfrak{m}$ teilbar ist. Das kann aber nur vorkommen, wenn $\mathfrak{m}$ ein Teiler von 2 oder von 3 ist. Also:

5. **Der Grad der Funktion $T_\mathfrak{m}$ ist gleich der Anzahl $\psi(\mathfrak{m})$ (Bd. II, § 168) der nach dem Modul $\mathfrak{m}$ inkongruenten, zu $\mathfrak{m}$ teilerfremden Zahlen in Ω, geteilt durch die Anzahl der nach $\mathfrak{m}$ inkongruenten Einheiten in Ω.**

Die Wurzeln der Funktion $T_\mathfrak{m}$ bestimmen einen algebraischen Körper $\mathfrak{T}_\mathfrak{m}$ über dem Klassenkörper, dessen relativer Grad höchstens gleich dem Grade von $T_\mathfrak{m}$ ist, und beide Grade sind gleich, wenn $T_\mathfrak{m}$ irreduzibel ist.

6. **Diesen Körper $\mathfrak{T}_\mathfrak{m}$ wollen wir den Teilungskörper für den Modul $\mathfrak{m}$ nennen.**

Diese Teilungskörper spielen für den Körper Ω eine ähnliche Rolle, wie die Kreisteilungskörper für den Körper der rationalen Zahlen, nur daß sich hier noch der Klassenkörper dazwischen schiebt, zu dem es im Körper der rationalen Zahlen, ebenso wie in jedem einklassigen Körper, kein Analogon gibt.

Nach dem Multiplikationstheorem (§ 151) kann

(9) $$\tau(\xi u) = \theta_\xi[\tau(u)]$$

rational durch $\tau(u)$ ausgedrückt werden. Setzen wir $u = \xi' \frac{\alpha}{\mu}$, so folgt:

(10) $$\tau_{\xi\xi'} = \tau\left(\frac{\xi\,\xi'\,\alpha}{\mu}\right) = \theta_\xi(\tau_{\xi'}),$$

und folglich durch Vertauschung von ξ mit ξ':

$$\theta_\xi(\tau_{\xi'}) = \theta_{\xi'}(\tau_\xi), \tag{11}$$

und damit nach Bd. I, § 169:

7. Der Teilungskörper ist in bezug auf den Klassenkörper relativ Abelsch.

Die Zahlen ξ, nach dem Modul $\mathfrak{m}$ genommen, bilden bei der Multiplikation eine Gruppe, und die Relativgruppe des Teilungskörpers ist mit dieser Gruppe isomorph (oder wenigstens mit einem Teiler dieser Gruppe. Die Irreduzibilität von $T_\mathfrak{m}$ wird weiterhin bewiesen werden, wodurch dann die Gruppe von $\mathfrak{T}_\mathfrak{m}$ selbst festgestellt ist).

§ 155. Multiplikation der elliptischen Funktionen für einen ungeraden Multiplikator.

Für den Nachweis der Existenz des Teilungskörpers ist die Benutzung der Weierstrassschen Funktion und der daraus abgeleiteten τ-Funktion sehr zweckmäßig, und es wäre am bequemsten, wenn man darauf auch die weitere Untersuchung dieses Körpers gründen könnte. Dafür aber ist die arithmetische Natur der Multiplikationsformeln noch nicht genügend bekannt, und es ist darum zurzeit noch notwendig, die komplexe Multiplikation und Teilung auch der Jacobischen elliptischen Funktionen zu betrachten.

Hierbei wollen wir den Multiplikationsformeln, die wir in § 57 abgeleitet haben, noch eine etwas andere Gestalt geben.

Wir betrachten zunächst durchweg den Multiplikator m als ungerade Zahl. Wir setzen, wenn

$$\varkappa = \frac{\vartheta_{10}}{\vartheta_{00}} \tag{1}$$

den Modul der elliptischen Funktionen bedeutet, nach Kronecker[1]):

$$\lambda = 4\left(\varkappa + \frac{1}{\varkappa}\right) = 4\frac{f(\omega)^4}{f_2(\omega)^4} + 4\frac{f_2(\omega)^4}{f(\omega)^4} \quad [\S\ 54,\ (3)], \tag{2}$$

und entwickeln diesen Ausdruck nach steigenden Potenzen von

$$q = e^{\pi i \omega}.$$

---

[1]) Zur Theorie der elliptischen Funktionen. Sitzungsbericht der Berliner Akademie vom 29. Juli 1886.

Man kann die Form dieser Entwickelung aus den Produktformeln [§ 24, (11)]:

$$\lambda = q^{-\frac{1}{2}} \Pi \left(\frac{1 + q^{2\nu - 1}}{1 + q^{2\nu}}\right)^4 + 16 q^{\frac{1}{2}} \Pi \left(\frac{1 + q^{2\nu}}{1 + q^{2\nu - 1}}\right)^4$$

ableiten, und findet:

(3) $$\lambda = q^{-\frac{1}{2}} (1 + \lambda_1 q + \lambda_2 q^2 + \lambda_3 q^3 + \cdots),$$

worin die Konstanten $\lambda_1, \lambda_2, \lambda_3, \ldots$ ganze rationale Zahlen sind.

Setzen wir ferner

(4) $$x = \sqrt{\varkappa} \operatorname{sn} \left(\frac{w}{\sqrt{\varkappa}}, \varkappa\right),$$

so bleibt (4) nach § 45, (9) ungeändert, wenn $\varkappa$ mit $1:\varkappa$ vertauscht wird. Es genügt x der Differentialgleichung

(5) $$\left(\frac{dx}{dw}\right)^2 = 1 - \tfrac{1}{4} \lambda x^2 + x^4.$$

Entwickelt man also x nach dem Taylorschen Lehrsatz in eine Reihe nach steigenden Potenzen von w:

(6) $$x = w + X_1 w^3 + X_2 w^5 \ldots,$$

so sind die Koeffizienten $X_1, X_2, \ldots$ ganze rationale Funktionen von λ mit rationalen Zahlenkoeffizienten, wie sich aus (5) nach der Methode der unbestimmten Koeffizienten ergibt.

Benutzt man die Bezeichnung von § 42, so ist

(7) $$x = \sqrt{\varkappa} \operatorname{sn} v = \frac{\vartheta_{11}(u)}{\vartheta_{01}(u)},$$

und nach § 57, IV. mit einer etwas modifizierten Bedeutung der A, B, C, D:

(8) $$\begin{aligned} \sqrt{\varkappa} \operatorname{sn} m v &= \frac{x A(x)}{D(x)}, \\ \operatorname{cn} m v &= \sqrt{1 - \frac{x^2}{\varkappa}} \frac{B(x)}{D(x)}, \\ \operatorname{dn} m v &= \sqrt{1 - \varkappa x^2} \frac{C(x)}{D(x)}. \end{aligned}$$

Hier sind $A(x)$, $B(x)$, $C(x)$, $D(x)$ ganze rationale Funktionen von x vom Grade $\frac{1}{2}(m^2 - 1)$, und es ist aus den Rekursionsformeln § 57, (13), (14) zu ersehen, daß die Funktionen A, D und das Produkt $B\,C$ ganze rationale Funktionen von λ sind, deren

Zahlenkoeffizienten rational sind. Daß es ganze Zahlen sind, ist wegen des Nenners 2, der zunächst auftritt, nicht zu ersehen.

Um dies näher zu untersuchen, betrachten wir die Wurzeln der Funktion $A(x)$: Sie sind, wenn gesetzt wird:

$$\Omega_{h,h'} = \frac{2hK + 2h'iK'}{m},$$

$$(9) \qquad x_{h,h'} = \sqrt{\varkappa}\,\mathrm{sn}\,\Omega_{h,h'} = \frac{\vartheta_{11}\left(\frac{h + h'\omega}{m}, \omega\right)}{\vartheta_{01}\left(\frac{h + h'\omega}{m}, \omega\right)},$$

worin h, h' irgend welche ganze Zahlen sein können; nur dürfen sie nicht beide gleich Null sein. Man erhält alle Wurzeln von $A(x)$, wenn man h, h' je ein volles Restsystem nach dem Modul m durchlaufen läßt, abgesehen von der Kombination 0,0. Es ist dann

$$(10) \quad x_{h,h'} = \frac{-i\sum\limits_{-\infty,\infty}^{\nu}(-1)^{\nu}\, e^{\frac{\pi i h}{m}(2\nu+1)}\, q^{\left(\frac{2h+1}{2}+\frac{h'}{m}\right)^2}}{\sum\limits_{-\infty,\infty}^{\nu}(-1)^{\nu}\, e^{\frac{2\pi i\nu h}{m}}\, q^{\left(\nu+\frac{h'}{m}\right)^2}}.$$

Um diesen Ausdruck nach steigenden Potenzen von q zu entwickeln, muß man zunächst die niedrigste Potenz von q im Nenner aufsuchen, d. h. das Glied, in dem $\nu + \frac{h'}{m}$ so klein als möglich wird. Dies findet statt, wenn ν die zunächst an $-h'/m$ gelegene ganze Zahl ist. Es gibt, da m ungerade ist, nur eine solche Zahl ν, und die Formel (10) erhält die Gestalt:

$$(11) \qquad x_{h,h'} = \frac{Q_1}{1 + Q_2} = Q_1 - Q_1 Q_2 + Q_1 Q_2^2 - \ldots,$$

worin Q_1 und Q_2 nach steigenden Potenzen von q geordnete Reihen sind, deren Koeffizienten ganze algebraische Zahlen (Kreisteilungszahlen) sind.

Demnach läßt sich $x_{h,h'}$ nach steigenden Potenzen von q entwickeln und die Koeffizienten dieser Entwickelung sind ganze algebraische Zahlen.

Ist S eine symmetrische Funktion der $x_{h,h'}$ mit rationalen ganzzahligen Koeffizienten, so läßt auch diese sich in derselben Weise nach Potenzen von q entwickeln. Andererseits ist S nach dem Fundamentalsatz über symmetrische Funktionen rational durch

die Koeffizienten von $A(x)$ ausdrückbar, ist also eine ganze rationale Funktion von λ mit rationalen Zahlenkoeffizienten von der Form:

$$(12) \qquad S = S_0 \lambda^s + S_1 \lambda^{s-1} + S_2 \lambda^{s-2} + \cdots + S_s,$$

worin die $S_0, S_1, S_2, \ldots,$ rationale Zahlen sind. Daß es ganze Zahlen sind, soll eben bewiesen werden. Das ergibt sich aber sehr einfach, wenn man in (12) für λ die Entwickelung (3) einsetzt und dann die Koeffizienten gleich hoher Potenzen von q auf beiden Seiten miteinander vergleicht. Man bekommt nämlich zur Bestimmung der $S_0, S_1, S_2, \ldots,$ eine Reihe linearer Gleichungen, deren jede folgende nur ein neues S_i und zwar mit dem Koeffizienten 1 enthält, während auf der anderen Seite dieser Gleichungen ganze algebraische Zahlen stehen. Hiernach sind also die $S_0, S_1, S_2, \ldots,$ ganze algebraische Zahlen, und da sie rational sind, sind es auch ganze rationale Zahlen.

Da wir überdies nach § 57, II und (7) $A(0)$ und $A(\infty)$ kennen, so ergibt sich für $A(x)$ der Ausdruck:

$$(13) \quad A(x) = \pm x^{m^2-1} + a_1 x^{m^2-3} + a_2 x^{m^2-5} + \cdots + m,$$

worin die $a_1, a_2, \ldots,$ ganze ganzzahlige Funktionen von λ sind.

Ferner ist nach § 57, (7):

$$D(x) = \pm x^{m^2-1} A\left(\frac{1}{x}\right),$$

und folglich:

$$(14) \quad \pm D(x) = \pm 1 + a_1 x^2 + a_2 x^4 + \cdots + m x^{m^2-2}.$$

[Das Zeichen $\pm$ in (13) und (14) ist nach § 57 bestimmt durch $(-1)^{\frac{m-1}{2}}$].

Für die Funktionen B und C gilt die Relation:

$$(15) \qquad B(x) = x^{m^2-1} C\left(\frac{1}{x}\right),$$

und ihre Wurzeln sind daher zueinander reziprok. Der erste und der letzte Koeffizient sind in B und in C gleich der Einheit.

Die Wurzeln von B sind:

$$y_{h,h'} = \sqrt{\varkappa}\ \mathrm{sn}(\Omega_{h,h'} + K) = \sqrt{\varkappa}\ \frac{\mathrm{cn}\,\Omega_{h,h'}}{\mathrm{dn}\,\Omega_{h,h'}}$$

$$(16) \qquad = \frac{\vartheta_{10}\left(\frac{h + h'\omega}{m}, \omega\right)}{\vartheta_{00}\left(\frac{h + h'\omega}{m}, \omega\right)}$$

und lassen sich in folgender Weise entwickeln:

$$(17) \qquad \frac{\overset{\nu}{\Sigma}\, q^{\left(\nu+\frac{1}{2}+\frac{h'}{m}\right)^2} e^{\frac{(2\nu+1)\pi i}{m} h}}{\overset{\nu}{\Sigma}\, q^{\left(\nu+\frac{h'}{m}\right)^2} e^{\frac{2\nu\pi i}{m} h}}.$$

Im Nenner dieses Ausdruckes kommt nur ein Glied mit niedrigster Potenz von q vor, das man erhält, wenn man für ν die dem Bruch $-h'/m$ zunächst gelegene ganze Zahl setzt.

Im Zähler kommt im allgemeinen auch nur ein niedrigstes Glied vor, dessen Koeffizient eine Einheit ist. In dem besonderen Falle, wo h'/m eine ganze Zahl ist, kommen aber im Zähler zwei gleiche niedrigste Glieder vor, nämlich (für $h' = 0$) $\nu = 0, -1$. Diese geben zusammen

$$q^{\frac{1}{4}}\, 2 \cos \frac{h\pi}{m}$$

und $2 \cos \frac{h\pi}{m}$ ist eine algebraische Einheit. [Zu schließen aus Bd. I, § 144, (19).]

Demnach läßt sich sowohl der Ausdruck (17), als auch sein reziproker Wert nach steigenden Potenzen von q in der Art entwickeln, daß der Koeffizient des ersten Gliedes den Wert 1 hat und alle übrigen Koeffizienten ganze algebraische Zahlen sind. Daraus schließt man, ebenso wie in bezug auf $A(x)$, daß sich $B(x)\, C(x)$ in der Weise darstellen läßt:

$$(18) \qquad B(x)\, C(x) = x^{2m^2-2} + b_1 x^{2m^2-4} + \cdots + 1,$$

worin die $b_1, b_2 \ldots$ ganze rationale Funktionen von λ mit ganzen rationalen Zahlenkoeffizienten sind. Außerdem sind die Koeffizienten b, die gleichweit vom Anfang und vom Ende abstehen, einander gleich.

Betrachten wir noch die aus (8) fließende Gleichung:

$$(19) \qquad x A(x) - \sqrt{\varkappa}\, \mathrm{sn}\, m v\, D(x) = 0,$$

die in bezug auf x vom Grade m^2 ist. Ihre Wurzeln sind die Größen:

$$\sqrt{\varkappa}\, \mathrm{sn}\, v, \quad \sqrt{\varkappa}\, \mathrm{sn}(v + \Omega_{h,h'}).$$

Das Produkt dieser Wurzeln ist, vom Vorzeichen abgesehen, gleich dem unabhängigen Gliede in dieser Gleichung, also gleich

$$\pm \sqrt{\varkappa}\, \mathrm{sn}\, m v,$$

und daraus ergibt sich:

$$(20) \qquad \pm \frac{\sqrt{\varkappa}\, \mathrm{sn}\, m v}{\sqrt{\varkappa}\, \mathrm{sn}\, v} = \overset{h,h'}{\Pi} \sqrt{\varkappa}\, \mathrm{sn}(v + \Omega_{h,h'}).$$

§ 156. Übergang zu den singulären Moduln.

Wir nehmen jetzt an, daß ω die Wurzel einer quadratischen Gleichung:

$$(1) \qquad a\omega^2 + b\omega + c = 0$$

mit der negativen Stammdiskriminante

$$(2) \qquad \varDelta = b^2 - 4ac$$

sei.

Ist dann $j(\omega)$ die Invariante, so genügt die Größe λ [§ 155, (2)] der Gleichung 6ten Grades:

$$(3) \quad \lambda^6 - 9.16\lambda^4 - [j(\omega) - 27.2^8]\lambda^2 + 64[j(\omega) - 27.64] = 0,$$

deren Koeffizienten ganze algebraische Zahlen sind. Folglich ist λ selbst eine ganze algebraische Zahl (Bd. II, § 154, 11.)[1] und in § 135 haben wir gesehen, daß λ Klasseninvariante der Diskriminante $4\varDelta$ oder $16\varDelta$ ist.

Wir adjungieren also dem Klassenkörper $\mathfrak{K}(\varDelta)$ die Zahl λ und erhalten einen Klassenkörper:

$$(4) \quad \begin{aligned} \mathfrak{L} &= \mathfrak{K}(4\varDelta), \quad \text{wenn } \varDelta \equiv 0 \pmod 4, \text{ oder } \equiv 1 \pmod 8. \\ \mathfrak{L} &= \mathfrak{K}(16\varDelta), \qquad\quad \varDelta \equiv 5 \pmod 8. \end{aligned}$$

Ist h die Klassenzahl von $\varDelta$, also der Relativgrad von $\mathfrak{K}(\varDelta)$ in bezug auf den quadratischen Körper $\Omega = \Re(\sqrt{\varDelta})$, und h' der Relativgrad von $\mathfrak{L}$ in bezug auf Ω, so ist (§ 100, § 123):

$$(5) \quad \begin{aligned} h' &= h, \ \text{wenn } \varDelta \equiv 1 \pmod 8, \\ h' &= 2h, \quad „ \quad \varDelta \equiv 0 \pmod 4, \\ h' &= 6h, \quad „ \quad \varDelta \equiv 5 \pmod 8. \end{aligned}$$

In dem ersten dieser drei Fälle ist also $\mathfrak{L}$ mit $\mathfrak{K}(\varDelta)$ identisch.

Durch die Substitution des singulären Moduls ω gehen die Koeffizienten $a_1, a_2 \ldots, b_1, b_2, \ldots,$ in § 155, (13), (18) in ganze algebraische Zahlen über, und daraus folgt, Bd. II, § 154, 11., daß die Wurzeln von $A(x)$, nämlich:

$$(6) \qquad \sqrt{\varkappa}\,\mathrm{sn}\,\Omega_{h,h'}, \ \text{ganze Zahlen}$$

und die Wurzeln von $B(x)$:

$$(7) \qquad \sqrt{\varkappa}\,\frac{\mathrm{cn}\,\Omega_{h,h'}}{\mathrm{dn}\,\Omega_{h,h'}}, \ \text{Einheiten}$$

sind.

[1] Dieser Umstand ist es, der die Einführung von λ an Stelle von $\varkappa$ besonders empfiehlt, weil $\varkappa$ im allgemeinen keine ganze Zahl ist, sondern erst $4\varkappa$.

Nun ist für variable $\varkappa$ und v [§ 45, (5)]:

$$\operatorname{dn}(v, \varkappa) = \frac{\operatorname{dn}(iv, \varkappa')}{\operatorname{cn}(iv, \varkappa')}. \tag{8}$$

Setzen wir hierin:

$$v = \Omega_{h,h'} = \frac{2hK + 2h'iK'}{m},$$

$$iv = \frac{-2h'K' + 2hiK}{m} = \Omega'_{-h',h},$$

so haben die Ω' dieselbe Bedeutung für $\varkappa'$ wie die Ω für $\varkappa$, d. h. sie entsprechen der Vertauschung von $(\omega, -1/\omega)$ und es ergibt sich aus (7) und (8), daß auch

$$\frac{\operatorname{dn}\Omega_{h,h'}}{\sqrt{\varkappa'}} \text{ eine Einheit ist.}$$

Es sind also auch

$$\frac{1}{\sqrt{\varkappa'}} \operatorname{dn}\Omega_{h,h'} = \frac{\vartheta_{00}\left(\frac{h + h'\omega}{m}\right)}{\vartheta_{01}\left(\frac{h + h'\omega}{m}\right)},$$

$$\sqrt{\frac{\varkappa}{\varkappa'}} \operatorname{cn}\Omega_{h,h'} = \frac{\vartheta_{10}\left(\frac{h + h'\omega}{m}\right)}{\vartheta_{01}\left(\frac{h + h'\omega}{m}\right)} \text{ algebraische Einheiten.} \tag{9}$$

Aus der Formel § 155, (20) folgt für $v = 0$:

$$\pm m = \overset{h,h'}{\Pi} \sqrt{\varkappa} \operatorname{sn}\Omega_{h,h'} = \Pi x_{h,h'}. \tag{10}$$

1. Die ganzen Zahlen $x_{\mu,\mu'}$ sind also Teiler der Zahl m.

Wir setzen jetzt, wenn m und n zwei ungerade Zahlen sind:

$$\Omega_{h,h'} = \frac{2hK + 2h'iK'}{m},$$

$$H_{l,l'} = \frac{2lK + 2l'iK'}{n},$$

und substituieren in der Formel § 155, (20):

$$v = H_{l,l'}.$$

Dadurch ergibt sich:

$$\frac{\sqrt{\varkappa} \operatorname{sn} m H_{l,l'}}{\sqrt{\varkappa} \operatorname{sn} H_{l,l'}} = \overset{h,h'}{\Pi} \sqrt{\varkappa} \operatorname{sn}(H_{l,l'} + \Omega_{h,h'}), \tag{11}$$

worin

$$H_{l,l'} + \Omega_{h,h'} = \frac{2(lm + hn)K + 2(l'm + h'n)iK'}{mn},$$

und folglich sind die Faktoren des Produktes (11):

$$\sqrt{\varkappa}\,\mathrm{sn}\,(H_{l,l'} + \Omega_{h,h'})$$

ganze Zahlen [nach (6)]. Vertauscht man in (11) wieder m und n, so folgt:

$$\text{(12)} \qquad \frac{\sqrt{\varkappa}\,\mathrm{sn}\,n\,\Omega_{h,h'}}{\sqrt{\varkappa}\,\mathrm{sn}\,\Omega_{h,h'}} \text{ ist eine ganze Zahl.}$$

Dies gilt für beliebige ungerade n, also auch, wenn n relativ prim zu m ist, für n^{-1} (mod m) und es ist also auch

$$\frac{\sqrt{\varkappa}\,\mathrm{sn}\,n^{-1}\,\Omega_{h,h'}}{\sqrt{\varkappa}\,\mathrm{sn}\,\Omega_{h,h'}} \text{ eine ganze Zahl.}$$

Ersetzt man hierin h, h' durch nh, nh', so folgt, daß auch

$$\frac{\sqrt{\varkappa}\,\mathrm{sn}\,\Omega_{h,h'}}{\sqrt{\varkappa}\,\mathrm{sn}\,n\,\Omega_{h,h'}} \text{ eine ganze Zahl ist,}$$

also ist der Quotient (12) eine Einheit, oder anders ausgedrückt:

2. Durchläuft n eine Reihe ungerader, zu m teilerfremder Zahlen, so sind die ganzen Zahlen:

$$\text{(13)} \qquad \sqrt{\varkappa}\,\mathrm{sn}\,n\,\Omega_{h,h'}$$

miteinander assoziiert.

§ 157. Komplexe Multiplikatoren.

Es genüge ω wie im vorigen Paragraphen der quadratischen Gleichung

$$\text{(1)} \qquad a\omega^2 + b\omega + c = 0$$

mit negativer Stammdiskriminante

$$\Delta = b^2 - 4ac,$$

also sei:

$$\text{(2)} \qquad \omega = \frac{-b + \sqrt{\Delta}}{2a}.$$

Wir legen unseren Betrachtungen wie im vorigen Paragraphen die Funktion

$$\text{(3)} \qquad \sqrt{\varkappa}\,\mathrm{sn}\,v = \frac{\vartheta_{11}(u)}{\vartheta_{01}(u)} = \boldsymbol{s}(u)$$

zugrunde, die wir als Funktion von $u = v/2K$ mit $\boldsymbol{s}(u)$ bezeichnen. Diese Funktion hat dann die durch

(4)
$$\boldsymbol{s}(u + 1) = -\boldsymbol{s}(u),$$
$$\boldsymbol{s}(u + \omega) = \boldsymbol{s}(u)$$

ausgedrückte doppelte Periodizität. Alle Perioden von $\boldsymbol{s}(u)$ sind in der Form $2m + n\omega$ enthalten, worin m, n ganze rationale Zahlen sind, und gehen also durch Multiplikation mit a in ganze Zahlen über.

Zwei Zahlen u, u', die sich nur um eine Periode unterscheiden, heißen kongruent nach dem Modul 2, ω:

$$u' \equiv u \pmod{2, \omega}.$$

Da die Funktion sn$v$ einen Wert nur zweimal im Periodenparallelogramm annimmt, so wird nur dann

$$\boldsymbol{s}(u) = \boldsymbol{s}(u'),$$

wenn entweder

(5)
$$u \equiv u' \quad \text{oder} \quad u \equiv 1 - u' \pmod{2, \omega}$$

ist, und $\boldsymbol{s}(u)$ verschwindet nur, wenn

$$u \equiv 0, 1 \pmod{2, \omega}$$

ist.

Da jede gebrochene Zahl in Ω durch Multiplikation mit einer ganzen rationalen Zahl in eine ganze Zahl verwandelt werden kann, so ergibt sich aus § 156, (6) der Satz:

1. Ist η irgend eine gebrochene Zahl des Körpers Ω, so ist $\boldsymbol{s}(\eta)$ eine algebraische Zahl, und wenn insbesondere η so dargestellt werden kann, daß sein Nenner relativ prim zu 2 ist, so ist $\boldsymbol{s}(\eta)$ eine ganze algebraische Zahl.

Es sei jetzt

(6)
$$\mu = y + x\sqrt{\Delta}$$

eine ganze Zahl in Ω, in der x, y ganze rationale Zahlen sind [1]), und

$$\mu' = y - x\sqrt{\Delta},$$

die zu μ konjugierte Zahl. Ferner

(7)
$$m = \mu\mu' = y^2 - \Delta x^2$$

die Norm von μ, die wir als ungerade voraussetzen.

---

[1]) Im Fall eines geraden Δ kann hiernach μ jede ganze Zahl aus Ω sein. Im Fall eines ungeraden Δ ist μ eine Zahl der Ordnung [2].

Es ist dann nach (2)

$$(8)\qquad \begin{aligned} \mu &= y + bx + 2a\omega x, \\ \mu\omega &= -2cx + (y - bx)\omega, \\ m &= (y + bx)(y - bx) + 4acx^2, \end{aligned}$$

woraus folgt, daß

$$y + bx \text{ und } y - bx$$

ungerade sind.

Daraus ergibt sich nach (4):

$$(9)\qquad \begin{aligned} \boldsymbol{s}[\mu(u + 1)] &= -\boldsymbol{s}(\mu u), \\ \boldsymbol{s}[\mu(u + \omega)] &= \boldsymbol{s}(\mu u). \end{aligned}$$

Die Funktion $\boldsymbol{s}(\mu u)$ hat also dieselben Perioden wie $s(u)$, und da $\boldsymbol{s}(\mu u)$ eine ungerade Funktion von u ist, so kann sie rational durch $\boldsymbol{s}(u)$ ausgedrückt werden. Wir bezeichnen mit $A(\boldsymbol{s})$, $D(\boldsymbol{s})$ ganze rationale Funktionen von $\boldsymbol{s} = \boldsymbol{s}(u)$, die übrigens nur die geraden Potenzen von $\boldsymbol{s}$ enthalten, und setzen:

$$(10)\qquad \boldsymbol{s}(\mu u) = \mu \boldsymbol{s}(u)\frac{A(\boldsymbol{s})}{D(\boldsymbol{s})}.$$

Die Werte von $\boldsymbol{s}(u)$, für die $\boldsymbol{s}(\mu u)$ Null oder unendlich wird, sind nach 3. algebraische Zahlen, und da sich aus diesen die Koeffizienten von A und D zusammensetzen lassen, so sind diese auch algebraische Zahlen. Um ihre Natur näher zu bestimmen, denken wir uns den Bruch (10) zunächst so erweitert, daß D rationale Koeffizienten erhält. Das geschieht dadurch, daß wir Zähler und Nenner mit dem Produkt aller zum Nenner konjugierten Faktoren multiplizieren. Wir können also $A(\boldsymbol{s})$ und $D(\boldsymbol{s})$ in die Form setzen:

$$(11)\qquad \begin{aligned} A(\boldsymbol{s}) &= A_1 + A_3\boldsymbol{s}^2 + A_5\boldsymbol{s}^4 + \cdots, \\ D(\boldsymbol{s}) &= D_1 + D_3\boldsymbol{s}^2 + D_5\boldsymbol{s}^4 + \cdots, \end{aligned}$$

worin die $D_1, D_3, \ldots,$ nach unserer Voraussetzung rationale Zahlen sind, während $A_1, A_3, \ldots,$ zu bestimmen sind. Setzen wir wie in § 155, (4), (6):

$$w = \sqrt{\varkappa}\, v = 2\sqrt{\varkappa}\, K u,$$

so geht $\boldsymbol{s}(u)$ in $\sqrt{\varkappa}\operatorname{sn}\left(\frac{w}{\sqrt{\varkappa}}\right)$ über, und die Gleichung (10) ergibt:

$$(12)\qquad \frac{D\left[\sqrt{\varkappa}\operatorname{sn}\left(\frac{\omega}{\sqrt{\varkappa}}\right)\right]\sqrt{\varkappa}\operatorname{sn}\left(\mu\frac{w}{\sqrt{\varkappa}}\right)}{\mu\operatorname{sn}\left(\frac{w}{\sqrt{\varkappa}}\right)} = A_1 + A_3\boldsymbol{s}^2 + A_5\boldsymbol{s}^4 + \cdots$$

Entwickelt man die linke Seite nach Potenzen von w, so sind die Koeffizienten rational durch λ und $\sqrt{\Delta}$ ausdrückbar, gehören also dem Körper

$$\mathfrak{L} = \mathfrak{R}(\lambda, \sqrt{\Delta})$$

an. Entwickelt man die rechte Seite in gleicher Weise und ordnet nach den Potenzen von w, so tritt A_ν zuerst in dem Koeffizienten von $w^{\nu-1}$ auf, und zwar mit dem Faktor 1 behaftet. Danach läßt sich A_ν bestimmen, wenn die früheren Koeffizienten schon bestimmt sind, und es folgt, daß alle diese Koeffizienten dem Körper $\mathfrak{L}$ angehören.

Da man nachträglich wieder Zähler und Nenner des Bruches A/D durch rationale Rechnung von gemeinschaftlichen Faktoren befreien kann, so ergibt sich der Satz:

2. Wenn in dem Ausdruck (8) Zähler und Nenner $A(\mathfrak{s})$, $D(\mathfrak{s})$ von gemeinschaftlichen Faktoren befreit sind, so gehören diese Funktionen dem Körper $\mathfrak{L}$ an.

Um die Funktion $A(x)$ darzustellen, nehmen wir den Koeffizienten der höchsten Potenz von x gleich 1 an und untersuchen, für welche Werte von u die Funktion $\mathfrak{s}(\mu u)$ verschwindet. Wir bezeichnen einen Wert u, für den $\mathfrak{s}(\mu u)$ verschwindet, mit $2\varrho/\mu$ und erhalten dann als Bedingung des Verschwindens nach (5) eine der beiden Kongruenzen

$$2\varrho \equiv 0, 1 \pmod{2, \omega}.$$

Es ist also ϱ eine Zahl des Körpers Ω, die zwar gebrochen sein, aber keine anderen Nenner als einen Teiler von $2a$ haben kann. Andererseits kann man ϱ um ein Vielfaches von μ verändern, ohne daß der Wert $\mathfrak{s}(2\varrho/\mu)$ geändert wird, und da es nur auf den letzteren ankommt, und man der Kongruenz:

$$\varrho \equiv \frac{\xi}{2a} \pmod{\mu},$$

wenn ξ eine ganze Zahl in Ω ist, durch eine ganze Zahl ϱ genügen kann, so können wir ϱ als ganze Zahl annehmen, wenn wir voraussetzen, daß der erste Koeffizient a in (1) ungerade und relativ prim zu μ sei. Diese Annahme halten wir von jetzt an fest.

Lassen wir also ϱ ein vollständiges Restsystem nach dem Modul μ mit Ausschluß der Null durchlaufen, so erhalten wir alle Werte von $\mathfrak{s}$, für die $A(\mathfrak{s})$ verschwindet, in der Form:

$$\mathfrak{s}\left(\frac{2\varrho}{\mu}\right). \tag{13}$$

Es ist noch zu zeigen, daß von den Zahlen (13) keine zwei einander gleich sind. Wäre

$$\mathbf{s}\left(\frac{2\varrho}{\mu}\right) = \mathbf{s}\left(\frac{2\varrho'}{\mu}\right),$$

ohne daß $\varrho \equiv \varrho'$ (mod μ) wäre, so müßte nach (5)

$$\frac{2(\varrho + \varrho')}{\mu} \equiv 1 \pmod{2, \omega}$$

sein. Es müßte also $a(1 + \omega)$ durch 2 teilbar sein, also auch, wenn ω zu ω' konjugiert ist, $a(1 + \omega')$ durch 2 teilbar, und mithin

$$a(\omega - \omega') = \sqrt{\varDelta} \equiv 0 \pmod{2}.$$

Es wäre also $\varDelta$ durch 4 teilbar, und $\frac{1}{4}\varDelta = \frac{1}{4}a^2(\omega - \omega')^2$ wäre gleichfalls noch Diskriminante, was der Annahme widerspricht, daß $\varDelta$ Stammdiskriminante sei[1]). Hiernach sind die Größen (13), deren Anzahl $m - 1$ beträgt (Bd. II, § 165), alle voneinander verschieden, und es ergibt sich

$$(14)\qquad A(x) = \prod^{\varrho}\left[x - \mathbf{s}\left(\frac{2\varrho}{\mu}\right)\right].$$

Die Funktion $\mathbf{s}(u)$ genügt nach § 44, (20) der Gleichung:

$$\mathbf{s}\left(u + \frac{\omega}{2}\right) = \frac{1}{\mathbf{s}(u)},$$

und wegen (8) und (4):

$$\mathbf{s}\left[\mu\left(u + \frac{\omega}{2}\right)\right] = \frac{(-1)^{cx}}{\mathbf{s}(\mu u)},$$

und demnach ergibt sich aus (10), wenn man u durch $u + \frac{\omega}{2}$ ersetzt:

$$(15)\qquad \frac{(-1)^{cx}}{\mathbf{s}(\mu u)} = \frac{1}{\mathbf{s}(u)} \frac{A\left(\frac{1}{\mathbf{s}}\right)}{D\left(\frac{1}{\mathbf{s}}\right)} = \frac{(-1)^{cx} D(\mathbf{s})}{\mathbf{s}(u) A(\mathbf{s})},$$

$$(16)\qquad A(\mathbf{s})\, A\left(\frac{1}{\mathbf{s}}\right) = (-1)^{cx} D(\mathbf{s})\, D\left(\frac{1}{\mathbf{s}}\right).$$

1) Es müßte b gerade und $a - b + c$ durch 4 teilbar sein, und $\frac{1}{4}\varDelta = \left(\frac{b}{2} - a\right)^2 - a(a - b + c)$ wäre Diskriminante. Für eine beliebige Diskriminante D könnte man denselben Zweck erreichen, wenn man zum Zähler der Ausdrücke (13) eine Potenz von 2 als Faktor hinzufügte.

Da A und D ohne gemeinschaftliche Teiler sind, so ist für eine Variable x und eine Konstante h:

$$h\, x^{m-1} A\left(\frac{1}{x}\right) = D(x),$$

und indem man x durch $1/x$ ersetzt:

$$h\, A(x) = x^{m-1} D\left(\frac{1}{x}\right),$$

und nach (16):

$$h^2 = (-1)^{cx}.$$

Also ist

(17) $$D(x) = \varepsilon\, x^{m-1} A\left(\frac{1}{x}\right),$$

worin $\varepsilon = \pm 1$ oder $= \pm i$ ist. Das hängt nach (16) davon ab, ob cx gerade oder ungerade ist[1]).

Gebrauchen wir also wieder die Bezeichnung (10), jedoch jetzt unter der Voraussetzung, daß A und D ohne gemeinschaftliche Teiler sind, so ergibt sich:

(18) $$\varepsilon\, \mathbf{s}(\mu u) = \frac{A_1 \mathbf{s} + A_3 \mathbf{s}^3 + \cdots A_{m-2} \mathbf{s}^{m-2} + \mathbf{s}^m}{1 + A_{m-2} \mathbf{s}^2 + \cdots A_3 \mathbf{s}^{m-3} + A_1 \mathbf{s}^{m-1}},$$

und die $A_1, A_3, \ldots, A_{m-1}$ sind ganze Zahlen des Körpers $\mathfrak{K}$, denn sie sind die symmetrischen Grundfunktionen der ganzen Zahlen (13).

Im besonderen ergibt sich, wenn man $u = 0$ setzt:

(19) $$A_1 = \varepsilon \mu,$$

und daraus:

(20) $$\varepsilon \mu = \prod^{\varrho} \mathbf{s}\left(\frac{2\varrho}{\mu}\right).$$

Die $\mathbf{s}\left(\frac{2\varrho}{\mu}\right)$ sind also Teiler von μ.

Aus (10) folgt:

(21) $$\mathbf{s}\, A(\mathbf{s}) - \mathbf{s}(\mu u)\, D(\mathbf{s}) = 0,$$

und dies ist, wenn $\mathbf{s}(\mu u)$ als gegeben betrachtet wird, eine Gleichung für $\mathbf{s}(u)$ vom m^{ten} Grade, deren Wurzeln sind:

$$\mathbf{s}(u),\ \mathbf{s}\left(u + \frac{2\varrho}{\mu}\right).$$

---

[1]) Aus § 138 ergibt sich, daß i im Körper $\mathfrak{K}$ enthalten ist; (17) steht also nicht im Widerspruch mit dem Satze 2.

Das Produkt dieser Wurzeln ist also, da s^m den Koeffizienten 1 hat, gleich dem negativen unabhängigen Glied, d. h. es ist:

$$\varepsilon \frac{s(\mu u)}{s(u)} = \prod^{\varrho} s\left(u + \frac{2\varrho}{\mu}\right), \tag{22}$$

und daraus für $u = 0$ wie oben:

$$\varepsilon \mu = \prod^{\varrho} s\left(\frac{2\varrho}{\mu}\right). \tag{23}$$

Es sei jetzt η eine gebrochene Zahl in Ω mit dem ungeraden Idealnenner $\mathfrak{a}$; dann folgt aus (22), daß $s(\mu\eta)/s(\eta)$ eine ganze Zahl ist, wenn μ eine beliebige Zahl (6) in Ω ist. Nehmen wir μ relativ prim zu $\mathfrak{a}$ und setzen $\mu'\mu \equiv 1 \pmod{\mathfrak{a}}$, so können wir η durch $\mu'\eta$ ersetzen und finden, daß auch $s(\eta)/s(\mu'\eta)$ eine ganze Zahl ist, worin μ' ebenso beliebig ist wie μ. Folglich ist auch $s(\eta)/s(\mu\eta)$ eine ganze Zahl und mithin eine Einheit.

Wir haben also den Satz:

3. Ist η eine Zahl in Ω mit ungeradem Idealnenner, und durchläuft μ eine Reihe relativer Primzahlen zu $\mathfrak{a}$, so sind die Zahlen

$$s(\mu\eta)$$

miteinander assoziiert.

Noch eine weitere Folgerung ergibt sich daraus, wenn man in (22) $u = 2\varrho_1/\mu_1$ setzt:

$$\frac{s\left(\frac{2\mu\varrho_1}{\mu_1}\right)}{s\left(\frac{2\varrho_1}{\mu_1}\right)} = \prod^{\varrho} s\left(\frac{2\varrho_1}{\mu_1} + \frac{2\varrho}{\mu}\right). \tag{24}$$

Sind nun μ und ϱ_1 relativ prim zu μ_1, so ist die linke Seite nach 3. eine Einheit, und folglich müssen auch alle Faktoren der rechten Seite

$$s\left(\frac{2\varrho_1}{\mu_1} + \frac{2\varrho}{\mu_2}\right), \tag{25}$$

die ja ganze Zahlen sind, Einheiten sein.

Auf diese Form läßt sich aber jedes $s(\eta)$ bringen, wenn

$$\eta = \frac{\nu}{\mu}$$

eine gebrochene Zahl in Ω ist, in deren Nenner zwei verschiedene Primideale aufgehen, falls dieser Nenner ungerade ist. Denn man kann in diesem Falle den Nenner μ von η in zwei Ideale $\mathfrak{a}_1 \mathfrak{a}_2$

zerlegen, die zueinander relativ prim sind, und man kann dann zwei ungerade ganze Zahlen α_1, α_2 in Ω bestimmen, die zueinander relativ prim sind, von denen die eine durch $\mathfrak{a}_1$, die andere durch $\mathfrak{a}_2$ teilbar ist. Es ist dann $\eta\,\alpha_1\,\alpha_2$ eine ganze Zahl in Ω und man kann nach Bd. II, § 166, (4) zwei ganze Zahlen ϱ_1, ϱ_2 so bestimmen, daß

$$\frac{\nu\,\alpha_1\,\alpha_2}{\mu} = \varrho_1\,\alpha_2 + \varrho_2\,\alpha_1$$

und daher

$$s\left(\frac{2\,\nu}{\mu}\right) = s\left(\frac{2\,\varrho_1}{\alpha_1} + \frac{2\,\varrho_2}{\alpha_2}\right)$$

wird. Dies ist aber von der Form (25). Wir bekommen daraus den Satz:

4. Enthält eine gebrochene Zahl η in Ω mit ungeradem Nenner zwei oder mehr verschiedene Primfaktoren im Nenner, so ist $s(\eta)$ eine Einheit.

§ 158. Zerlegung der Funktion $A(x)$.

Es seien jetzt

$$(1)\qquad \begin{aligned} \mu &= y + x\sqrt{\Delta}, \\ \mu_1 &= y_1 + x_1\sqrt{\Delta} \end{aligned}$$

zwei ungerade ganze Zahlen in Ω von der Form § 157, (6). Es sei $\mathfrak{m}$ der größte gemeinschaftliche Idealteiler von μ und μ_1. Setzt man also

$$(2)\qquad \begin{aligned} \mu &= \mathfrak{m}\,\mathfrak{a}, \\ \mu_1 &= \mathfrak{m}\,\mathfrak{a}_1, \end{aligned}$$

so sind $\mathfrak{a}$ und $\mathfrak{a}_1$ zwei äquivalente Ideale ohne gemeinsamen Teiler.

Die den beiden Zahlen μ, μ_1 entsprechenden Funktionen $A(x)$ bezeichnen wir mit

$$A_\mu(x),\ A_{\mu_1}(x),$$

und fragen, welche gemeinschaftliche Wurzeln diese Funktionen haben, wann also die Gleichung:

$$(3)\qquad s\left(\frac{2\,\varrho}{\mu}\right) = s\left(\frac{2\,\varrho_1}{\mu_1}\right)$$

erfüllt sein kann, wenn ϱ nach dem Modul μ, ϱ_1 nach dem Modul μ_1 genommen ist.

Da die Kongruenz

$$\frac{2\varrho}{\mu} + \frac{2\varrho_1}{\mu_1} \equiv 1 \pmod{2, \omega}$$

nicht möglich ist, was man ganz wie oben (S. 589) zeigt, so ist für die Gleichung (3) notwendig und hinreichend:

$$(4) \qquad \frac{2(\mu_1 \varrho - \mu \varrho_1)}{\mu \mu_1} \equiv 0 \pmod{2, \omega}.$$

Daraus folgt:

$$(5) \qquad \mu \varrho_1 \equiv \mu_1 \varrho \pmod{\mu \mu_1},$$

und dies ist nur dann möglich, wenn

$$(6) \qquad \varrho \equiv 0 \pmod{\mathfrak{a}}, \quad \varrho_1 \equiv 0 \pmod{\mathfrak{a}_1}.$$

Sind umgekehrt die Bedingungen (5) und (6) erfüllt, so ist:

$$\frac{2\varrho}{\mu} - \frac{2\varrho_1}{\mu_1}$$

eine ganze Zahl und die Gleichung (3) ist befriedigt.

Man nehme nun eine durch $\mathfrak{a}$ teilbare ganze Zahl in Ω:

$$(7) \qquad \alpha = \mathfrak{a}\mathfrak{c},$$

worin $\mathfrak{c}$ relativ prim zu μ und μ_1 ist. Wenn dann ϱ durch $\mathfrak{a}$ teilbar ist, so kann man eine ganze Zahl ξ nach dem Modul $\mathfrak{m}$ aus der Kongruenz

$$\varrho \equiv \alpha \xi \pmod{\mu}$$

bestimmen (Bd. II, § 166, 7.); dann ist

$$(8) \qquad \alpha_1 = \frac{\alpha \mu_1}{\mu} = \mathfrak{a}_1 \mathfrak{c}$$

eine durch $\mathfrak{a}_1 \mathfrak{c}$ und durch kein anderes Ideal teilbare ganze Zahl, und aus (5) ergibt sich

$$\varrho_1 \equiv \alpha_1 \xi \pmod{\mu_1}.$$

5. Wir erhalten also die gemeinschaftlichen Wurzeln von $A_\mu(x)$, $A_{\mu_1}(x)$ in der Form:

$$(9) \qquad s\left(\frac{2\alpha\xi}{\mu}\right) = s\left(\frac{2\alpha_1\xi}{\mu_1}\right),$$

worin ξ ein vollständiges Restsystem nach dem Modul $\mathfrak{m}$ durchläuft.

Hierin kann $\mathfrak{m}$ jedes beliebige ungerade Ideal in Ω bedeuten.

Denn man kann zu jedem solchen Ideal zwei Zahlen μ, μ_1 von der Form (2) wählen und dann ω unter den äquivalenten Zahlen so, daß a ungerade und relativ prim zu $\mu\mu_1$ wird.

Sucht man den größten gemeinschaftlichen Teiler von A_μ und A_{μ_1}, so erhält man eine ganze Funktion $A_{\mathfrak{m}}$, deren Koeffizient ganze Zahlen in $\mathfrak{L}$ sind, deren Wurzeln die Größen (9) sind, und wenn man endlich $A_{\mathfrak{m}}$ von Faktoren befreit, die es mit irgend einem $A_{\mathfrak{m}'}$ gemein hat, in dem $\mathfrak{m}'$ ein echter Teiler von $\mathfrak{m}$ ist, so erhält man eine ganze Funktion:

$$(10) \qquad T_{\mathfrak{m}}(x) = x^\nu - \tau_{\nu-1} x^{\nu-1} + \tau_{\nu-2} x^{\nu-2} - \cdots \pm \tau_0,$$

deren Wurzeln nur die unter den Größen (8) sind, in denen ξ relativ prim zu $\mathfrak{m}$ ist.

Der Grad ν dieser Funktion ist nach Bd. II, § 168 zu bestimmen. Wir wollen sie die Idealteilungsfunktion nennen. Ihre Koeffizienten sind ganze Zahlen des Körpers $\mathfrak{L}$, und es ist speziell

$$(11) \qquad \tau_0 = \prod^{\xi} \mathbf{s}\left(\frac{2\,\alpha\,\xi}{\mu}\right),$$

worin ξ ein vollständiges System inkongruenter, zu m teilerfremder Zahlen durchläuft.

Die Wurzeln von $T_{\mathfrak{m}}(x)$ sind gleich und entgegengesetzt, und wir erhalten eine Gleichung von Graden $\frac{1}{2}\nu$ für die Größe

$$\mathbf{s}\left(\frac{2\,\alpha\,\xi}{\mu}\right)^2.$$

Durch Adjunktion dieser Größen zu dem Körper $\mathfrak{L}$ entsteht ein Körper $\mathfrak{T}_{\mathfrak{m}}$, den wir gleichfalls Teilungskörper nennen. Er ergibt sich aus dem Teilungskörper des § 154 durch Adjunktion von $\varkappa$. Die Gruppe dieses Körpers ist in der Gruppe der Zahlen ξ (mod $\mathfrak{m}$) enthalten, wie leicht aus den Multiplikationsformeln folgt.

Wir bemerken noch, daß sich der allgemeine Teilungskörper $\mathfrak{T}_{\mathfrak{m}}$ durch Anwendung des Additionstheorems auf den Fall zurückführen läßt, wo $\mathfrak{m}$ eine Potenz eines Primideals in Ω ist.

§ 159. Primideale.

6. Ist η eine gebrochene Zahl des Körpers Ω, die in reduzierter Form den ungeraden Idealnenner $\mathfrak{a}$ hat, und ist $\mathfrak{m}$ ein zu $\mathfrak{a}$ relativ primes Ideal, so ist die ganze Zahl $\mathbf{s}(\eta)$ relativ prim zu $\mathfrak{m}$.

Denn man nehme in Ω eine durch $\mathfrak{a}$ teilbare, zu $2\,\mathfrak{m}$ teilerfremde ganze Zahl μ an. Dann ist $\mu\,\eta$ eine ganze Zahl. In dem Produkt § 157, (23)

(1) $$\mu = \overset{\varrho}{\Pi}\, s\left(\frac{2\varrho}{\mu}\right)$$

kommt eine Zahl 2ϱ vor, die mit $\mu\eta$ nach dem Modul μ kongruent ist. Folglich ist $s(\eta)$ ein Teiler von μ und mithin relativ prim zu $\mathfrak{m}$, wie bewiesen werden sollte.

Nehmen wir jetzt an, daß in der Formel (11), § 158

(2) $$\tau_0 = \overset{\xi}{\Pi}\, s\left(\frac{2\alpha\xi}{\mu}\right)$$

$\mathfrak{m}$ ein Primideal des Körpers Ω sei und setzen demgemäß $\mathfrak{m} = \mathfrak{p}$, so daß ξ ein volles Restsystem nach dem Modul $\mathfrak{p}$ mit Ausschluß der Null durchläuft.

Nehmen wir dann μ so an, daß es nur durch die erste Potenz von $\mathfrak{p}$ teilbar und durch ein beliebig gewähltes anderes Primideal $\mathfrak{p}'$ nicht teilbar ist, so kann τ_0 nach dem Satz 6. nicht durch $\mathfrak{p}'$ teilbar sein. Nun ist τ_0 nur von dem Ideal $\mathfrak{p}$ abhängig und unabhängig davon, wie im übrigen die Zahl μ genommen ist. Folglich ist τ_0 nach dem Satz 6. durch kein von $\mathfrak{p}$ verschiedenes Primideal teilbar. Es kann aber auch $\mathfrak{p}$ nicht in einer höheren als der ersten Potenz in τ_0 aufgehen, denn die Faktoren des Produktes (1) kommen alle unter den Faktoren des Produktes (2) vor, und folglich ist μ durch τ_0 teilbar. Demnach können wir geradezu

(3) $$\tau_0 = \mathfrak{p}$$

setzen, und da τ_0 eine Zahl im Körper $\mathfrak{L}$ ist, so folgt:

7. Jedes ungerade Primideal des Körpers Ω ist ein Körper $\mathfrak{L}$, ein Hauptideal.

Auch in der Annahme, daß μ relativ prim zu a sein sollte, liegt keine Einschränkung dieses Satzes. Denn wir können bei gegebenem $\mathfrak{p}$ unter den äquivalenten Formen (a, b, c), ohne λ zu ändern, eine auswählen, bei dem diese Forderung erfüllt ist.

Noch nicht bewiesen ist aber hierdurch, daß $\mathfrak{p}$ auch im Klassenkörper $\mathfrak{K}(\Delta)$ selbst ein Hauptideal ist. Wenigstens folgt dies nur in dem Fall $\Delta \equiv 1 \pmod 8$, wo $\mathfrak{K}$ mit $\mathfrak{L}$ identisch ist[1]).

Nach dem Satz 3., § 157 sind die Faktoren des Produktes (2) alle miteinander assoziiert. Die Anzahl dieser Faktoren ist $N(\mathfrak{p}) - 1$, und demnach können wir auch setzen:

(4) $$\mathfrak{p} = \left[s\left(\frac{2\alpha}{\mu}\right)\right]^{N(\mathfrak{p})-1}.$$

[1]) Vgl. hierzu § 122, wo auch der Fall der Primzahl 2 erledigt ist.

§ 160. Primideale ersten Grades in $\mathfrak{T}_m$.

Es kommt nun vor allem darauf an, die Primzahlen p aufzusuchen, die im Körper $\mathfrak{K}$ in Primideale ersten Grades zerlegbar sind. Nach § 122 und § 156 sind das die Primzahlen p, die durch die Hauptform der Diskriminante $D = 4\Delta$ oder 16Δ darstellbar sind. Diese sind von der Form:

1) $p = y^2 - \Delta x^2, \quad \Delta \equiv 0 \pmod 4$ oder $\equiv 1 \pmod 8$,

2) $p = y^2 - 4\Delta x^2, \quad \Delta \equiv 5 \pmod 8$.

Ist $\Delta \equiv 1 \pmod 8$, so muß der dritte Koeffizient der Form (a, b, c) gerade sein. Ist $\Delta \equiv 0 \pmod 4$, so können wir c gerade annehmen, indem wir nötigenfalls zu der Parallelform $(a, b + 2a, a + b + c)$ übergehen. Zerfällt also p in die beiden Primfaktoren π, π', so ist

$$(1) \qquad \begin{aligned} &1) \quad \pi = y + x\sqrt{\Delta}, \\ &2) \quad \pi = y + 2x\sqrt{\Delta}, \end{aligned}$$

und um die Multiplikationsformel § 157, (10), (17) auf $\mu = \pi$ anzuwenden, haben wir im letzteren Falle x durch $2x$ zu ersetzen. Wir können also in allen Fällen cx gerade und daher $\varepsilon = \pm 1$ annehmen.

Die in den Darstellungen (1), 1), 2) liegenden Bedingungen für den Modul 2 lassen sich in die eine zusammenfassen:

$$\pi \equiv 1 \pmod 2.$$

Setzen wir, wenn $N(\pi) = p$ ist, für den Augenblick zur Abkürzung:

$$(2) \qquad \begin{aligned} \varphi(x) &= A_1 x + A_3 x^3 + \cdots + A_{p-2} x^{p-2} + x^p, \\ \psi(x) &= 1 + A_{p-2} x^2 + \cdots + A_3 x^{p-3} + A_1 x^{p-1}, \end{aligned}$$

so ist nach § 157, (18), (19)

$$(3) \qquad A_1 = \pm \pi,$$

und

$$(4) \qquad \pm \mathbf{s}(\pi u) = \frac{\varphi(\mathbf{s})}{\psi(\mathbf{s})},$$

und daraus ergibt sich durch Differentiation nach u:

$$(5) \qquad \pm \frac{\pi \mathbf{s}'(\pi u)}{\mathbf{s}'(u)} = \frac{\varphi'(\mathbf{s})\psi(\mathbf{s}) - \varphi(\mathbf{s})\psi'(\mathbf{s})}{\psi(\mathbf{s})^2}.$$

Nach § 155, (5) ist aber

$$\mathbf{s}'(u)^2 = 1 - \tfrac{1}{4}\lambda \mathbf{s}^2 + \mathbf{s}^4,$$

und aus (5) ergibt sich durch Quadrieren mit Benutzung von (4):

$$\pi^2 \frac{4\,\psi(\boldsymbol{s})^4 - \lambda\,\varphi(\boldsymbol{s})^2\psi(\boldsymbol{s})^2 + 4\,\psi(\boldsymbol{s})^4}{4 - \lambda\,\boldsymbol{s}^2 + 4\,\boldsymbol{s}^4} = [\varphi'(\boldsymbol{s})\psi(\boldsymbol{s}) - \varphi'(\boldsymbol{s})\psi(\boldsymbol{s})]^2.$$

Da rechts eine ganze Funktion von $\boldsymbol{s}$ steht, so muß auf der linken Seite der Zähler durch den Nenner teilbar sein (was sich auch aus der Betrachtung der Nullpunkte ergibt), und es folgt:

$$\pi^2 \Phi = [\varphi'(\boldsymbol{s})\,\psi(\boldsymbol{s}) - \varphi(\boldsymbol{s})\,\psi'(\boldsymbol{s})]^2,$$

wo Φ eine ganze Funktion von $\boldsymbol{s}$ ist, deren Koeffizienten ganze Zahlen in $\mathfrak{L}$ sind. Es muß also Φ das Quadrat einer ganzen Funktion sein, deren Koeffizienten gleichfalls ganze algebraische Zahlen sind (Bd. I, § 2; Bd. II, § 159), und es ergibt sich daraus für ein variables x:

(6) $$\varphi'(x)\,\psi(x) - \psi'(x)\,\varphi(x) \equiv 0 \pmod{\pi}.$$

Hiernach läßt sich beweisen, daß die Koeffizienten A_1, A_3, $A_5, \ldots, A_{p-2}$ alle durch π teilbar sind.

Von A_1 wissen wir das schon. Nehmen wir also an, es sei bewiesen für

$$A_1, A_3, \ldots, A_{2\nu-1} \quad (2\nu + 1 < p),$$

so folgt:

$$\left.\begin{aligned} \varphi\,(x) &\equiv A_{2\nu+1}\,x^{2\nu+1} + \cdots \\ \varphi'(x) &\equiv (2\nu+1)\,A_{2\nu+1}\,x^{2\nu} + \cdots \\ \psi\,(x) &\equiv 1 + A_{p-2}\,x^2 + \cdots \\ \psi'(x) &\equiv 2\,A_{p-2}\,x + \cdots \end{aligned}\right\} \pmod{\pi}$$

Suchen wir also in (6) den Koeffizienten von $x^{2\nu}$, so folgt:

$$(2\nu + 1)\,A_{2\nu+1} \equiv 0 \pmod{\pi}.$$

Da $2\nu + 1 < p$ und p eine Primzahl ist, so ist $2\nu + 1$ relativ prim zu π, und es folgt:

(7) $$A_{2\nu+1} \equiv 0 \pmod{\pi}.$$

Setzen wir in (4) für u einen der Werte $2\alpha\,\xi/\mu$, § 158, (9), so wird $\boldsymbol{s}(u)$ eine Wurzel der Ideal-Teilungsgleichung § 158, (10), und es folgt:

$$\pm\,\boldsymbol{s}(\pi u) \equiv [\boldsymbol{s}(u)]^p \pmod{\pi},$$

und wenn wir ein Quadrat erheben:

(8) $$\boldsymbol{s}(\pi u)^2 \equiv [\boldsymbol{s}(u)]^{2p} \pmod{\pi}.$$

Insbesondere ist also

(9) $$\boldsymbol{s}(u)^2 \equiv \boldsymbol{s}(u)^{2p} \pmod{\pi},$$

wenn

(10) $$\pi \equiv \pm 1 \pmod{m}$$

ist. Die Zahl $s(u)^2$ erzeugt den Körper $\mathfrak{T}_m$. Es ist außerdem nach § 122 für jede Zahl ϱ in $\mathfrak{L}$:

(11) $$\varrho \equiv \varrho^p \pmod{\mathfrak{P}},$$

wenn $\mathfrak{P}$ ein in π aufgehendes Primideal in $\mathfrak{L}$ ist, und folglich ist für jede ganze Zahl τ in $\mathfrak{T}_m$, wenn $\mathfrak{P}'$ ein Primideal in $\mathfrak{T}_m$ ist:

(12) $$\tau^p \equiv \tau \pmod{\mathfrak{P}'},$$

wenn die Bedingungen (10) und (1) erfüllt sind.

Daraus ergibt sich:

8. Damit eine in Ω existierende Primzahl π im Körper $\mathfrak{T}_m$ in Primideale ersten Grades zerfalle, ist notwendig und hinreichend, daß

$$\pi \equiv 1 \pmod{2},$$
$$\pi \equiv \pm 1 \pmod{m}.$$

Von einer gewissen endlichen Anzahl von Primzahlen (die in den Diskriminanten der auftretenden Gleichungen aufgehen) ist dabei abgesehen.

§ 161. Zahlgruppen und Idealgruppen.

Wie in § 98 und § 106 bezeichne ich mit O die Gesamtheit der ganzen und gebrochenen Zahlen des quadratischen Körpers Ω, nach Ausschluß aller Zahlen, die zu einem beliebig angenommenen S nicht teilerfremd sind. S kann eine rationale Zahl, eine Zahl in Ω oder auch ein Ideal sein. Ich will es den Exkludenten nennen. In den drei Abhandlungen „über Zahlgruppen in algebraischen Körpern" [1]) habe ich gewisse Systeme von Zahlen aus O unter dem Namen Zahlgruppen zusammengefaßt, die dadurch definiert waren, daß das Produkt und der Quotient je zweier Zahlen einer solchen Gruppe in derselben Gruppe enthalten waren. Eine solche Zahlgruppe kann niemals die Zahl Null enthalten, enthält aber sicher die Zahl 1 [2]).

Im gleichen Sinne wie von Zahlgruppen können wir auch von Idealgruppen reden, die ebenfalls ihren Exkludenten haben können. Es kommen hierbei natürlich auch gebrochene Ideale vor, und man bedient sich dabei nicht ohne Nutzen der Darstellungsweise durch die Funktionale (Bd. II, § 169).

[1]) Mathematische Annalen Bd. 48, 49, 50.

[2]) Fueter nennt diese Gruppen „Zahlstrahlen". Vgl. Fueter, Die Theorie der Zahlstrahlen I, II; Crelle, Bd. 130, 132.

Die Gesamtheit der ganzen und gebrochenen Zahlen des Körpers Ω, der wir einen beliebigen Exkludenten S beilegen, bildet die Zahlgruppe O und die Gesamtheit der Ideale $\overline{O}$ in dem gleichen Sinne eine Idealgruppe.

Ebenso bildet die Gesamtheit der numerischen Einheiten eine Zahlgruppe E und die Gesamtheit der funktionalen Einheiten eine Idealgruppe $\overline{E}$.

Die Multiplikation zweier Gruppen A und B zu dem Produkt AB geschieht dadurch, daß man jedes Element von A mit jedem Element von B multipliziert. Ist A eine Zahlgruppe, so ist $\overline{E}A$ eine Idealgruppe. Diese enthält aber nur Hauptideale und kann daher Hauptidealgruppe genannt werden.

Wenn die ganze Gruppe O in eine endliche Anzahl von Nebengruppen nach A zerfällt:

(1) $$O = A\alpha_1 + A\alpha_2 + \cdots + A\alpha_j,$$

so heißt die Zahl j der Index von A und wird mit

(2) $$j = (O, A)$$

bezeichnet (wie in § 100).

Wir sprechen den ersten Satz aus:

1. Ist A eine Zahlgruppe mit endlichem Index j, und η eine beliebige Zahl in O, so ist η^j in A enthalten.

Denn von der unbegrenzten Reihe der Potenzen $1, \eta, \eta^2, \eta^3, \ldots$, müssen zwei verschiedene Glieder in derselben Nebengruppe $A\alpha_i$ enthalten sein, und ihr Quotient, der ja auch eine Potenz von η ist, ist in A enthalten. Der niedrigste Exponent r, für den η^r in A enthalten ist, erweist sich in bekannter Weise als Teiler von j.

2. Ist A eine Zahlgruppe mit endlichem Index, so läßt sich auch die Idealgruppe $\overline{O}$ nach $\overline{E}A$ in eine endliche Zahl von Nebengruppen zerlegen:

(3) $$\begin{aligned} \overline{O} &= \overline{A}_1 + \overline{A}_2 + \cdots + \overline{A}_h, \\ &= A\mathfrak{a}_1 + A\mathfrak{a}_2 + \cdots + A\mathfrak{a}_h, \end{aligned}$$

und zwar können wir darin $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_h$ als ganze Ideale in $\overline{O}$ wählen, da wir jedes gebrochene Ideal in $\overline{O}$ nach 1. durch Multiplikation mit einer Zahl in A in ein ganzes Ideal verwandeln können. Wir brauchen nur für η eine Zahl zu wählen, die durch den Nenner des Ideals teilbar ist, und mit einer genügend hohen Potenz von η zu multiplizieren.

Die Zahl

(4) $$h = (\overline{O}, \overline{E}A)$$

heißt die Klassenzahl des Körpers Ω nach A, und das System $A\mathfrak{a}_1, A\mathfrak{a}_2, \ldots, A\mathfrak{a}_h$ die Idealklassen nach A. Den Satz 2. können wir nach den allgemeinen Gruppensätzen im § 100, 12. beweisen. Danach ist:

$$(\overline{O}, \overline{E}A) = (\overline{O}, \overline{E}O)\,(\overline{E}O, \overline{E}A),$$
$$(\overline{E}O, \overline{E}A) = (\overline{E}O, \overline{E}EA) = (O, EA),$$
$$(O, EA)\,(EA, A) = (O, A),$$
$$(EA, A) = (E, E'),$$

wenn E' die Gruppe der in A enthaltenen numerischen Einheiten bedeutet. Folglich ist

(5) $$(\overline{O}, \overline{E}A) = (\overline{O}, \overline{E}O)\,\frac{(O, A)}{(E, E')},$$

und $(\overline{O}, \overline{E}O)$ ist die Zahl der absoluten Idealklassen in Ω, also eine endliche Zahl. Die Zahl (E, E') ist im quadratischen Körper mit negativer Diskriminante gleich 1, wenn -1 in A vorkommt, gleich 2, wenn -1 nicht in A vorkommt, und kann nur in den beiden Ausnahmefällen $\Delta = -4$, $\Delta = -3$ bis zu 4 oder bis zu 6 ansteigen.

Gehören $\mathfrak{a}_1, \mathfrak{a}_1'$ einer Klasse $\overline{A}_1$ an, und $\mathfrak{a}_2, \mathfrak{a}_2'$ einer Klasse $\overline{A}_2$, so gehören die Produkte $\mathfrak{a}_1\mathfrak{a}_2$ und $\mathfrak{a}_1'\mathfrak{a}_2'$ in dieselbe Klasse, die wir die Klasse $\overline{A}_1\overline{A}_2$ nennen. Die Klassen lassen sich also komponieren und bilden eine endliche Abelsche Gruppe, in der die Hauptklasse $\overline{E}A$ die Einheit ist.

Eine Zahlgruppe A soll Kongruenzgruppe heißen, wenn sie nicht nur aus einzelnen Zahlen, sondern aus ganzen Zahlklassen nach einem Modul M besteht, d. h. wenn α zu A gehört, so sollen auch alle mit α nach dem Modul M kongruenten Zahlen zu A gehören; M soll der Modul der Kongruenzgruppe heißen. Eine Kongruenzgruppe hat immer einen endlichen Index, weil ja schon die Anzahl der Zahlklassen nach dem Modul M endlich ist. Statt M kann man auch jedes Vielfache von M als Modul wählen. Darum gewinnen wir auch keinen allgemeineren Begriff, wenn wir für M ein Ideal nehmen. Wir können sogar M als natürliche Zahl annehmen.

Wenn ein Ideal $\mathfrak{m}$ relativ prim zu M ist, so kann man in jeder durch α repräsentierten Zahlklasse eine Zahl α_0 aus der Kongruenz

(6) $$\alpha_0 = \alpha + M\vartheta \equiv 0 \pmod{\mathfrak{m}}$$
bestimmen, worin ϑ eine ganze Zahl in Ω ist.

Daraus folgt, daß jedes im Exkludenten aufgehende Primideal $\mathfrak{e}$ in M aufgehen muß, weil sonst α_0 für $\mathfrak{m} = \mathfrak{e}$ durch $\mathfrak{e}$ teilbar wäre.

Haben α und M einen gemeinschaftlichen Teiler, so haben alle Zahlen der Form $\alpha + M\xi$, in der ξ eine beliebige Zahl ist, denselben gemeinschaftlichen Teiler mit M. Es gibt aber in A auch Zahlen, die relativ prim zu M sind, z. B. die Zahl 1. Es gilt dann der folgende Satz:

3. Ist $\mathfrak{m}$ relativ prim zu M, so kann man in A eine durch $\mathfrak{m}$ teilbare ganze Zahl $\alpha_0 = \mathfrak{m}\mathfrak{n}$ von der Art bestimmen, daß $\mathfrak{n}$ zu M und einem beliebig gegebenen Ideal $\mathfrak{c}$ relativ prim wird.

Hat man nämlich nach (6) eine durch $\mathfrak{m}$ teilbare Zahl
$$\alpha_0 = \mathfrak{m}\mathfrak{n}$$
bestimmt, die zu M teilerfremd ist, so erhält man andere solche Zahlen:
$$\alpha_0' = \alpha_0 + M\xi = \mathfrak{m}\mathfrak{n}',$$
wenn
$$\xi = \mathfrak{m}\mathfrak{x}$$
eine beliebige durch $\mathfrak{m}$ teilbare ganze Zahl ist. Ist nun $\mathfrak{q}$ ein in $\mathfrak{c}$, aber nicht in α_0 aufgehendes Primideal, so nehme man $\mathfrak{x}$ durch $\mathfrak{q}$ teilbar an, dann ist $\mathfrak{n}'$ nicht durch $\mathfrak{q}$ teilbar. Geht aber $\mathfrak{q}$ in $\mathfrak{c}$ und in α_0 auf, so nehme man $\mathfrak{x}$ durch $\mathfrak{q}$ nicht teilbar an; dann ist auch $\mathfrak{n}'$ nicht durch $\mathfrak{q}$ teilbar.

Daraus folgt:

4. Ist $\mathfrak{m}$ ein beliebiges zu M teilerfremdes Ideal, so gibt es in jeder Idealklasse $\overline{A}_\nu$ Ideale, die zu $\mathfrak{m}$ relativ prim sind.

Man nehme, um dies zu beweisen, ein Ideal $\mathfrak{b}$ in der Klasse $(\overline{A}_\nu)^{-1}$ und bestimme nach 3. eine Zahl
$$\alpha = \mathfrak{a}\mathfrak{b},$$
so daß $\mathfrak{a}$ relativ prim zu $\mathfrak{m}$ ist, dann gehört $\mathfrak{a}$ in die Klasse $\overline{A}_\nu$ und genügt der Forderung des Satzes 4.

§ 162. Die durch ein Ideal teilbaren Ideale der Hauptklasse.

Es soll jetzt unter Ω der quadratische Körper mit negativer Grundzahl Δ verstanden werden.

In diesem Körper sei A eine Kongruenzgruppe mit dem Modul M und dem Exkludenten S. Die Gruppe A enthält, wie wir gesehen haben, unendlich viele ganze Zahlen. Wir fragen nach der Anzahl $T(t)$ der ganzen Zahlen in A, die durch irgend ein gegebenes ganzes zu M teilerfremdes Ideal $\mathfrak{m}$ teilbar sind, deren Norm nicht größer als die positive Zahl t ist.

Es sei (α_1, α_2) eine Basis von $\mathfrak{m}$, also nach § 91, (11):

$$(1) \qquad \alpha_1 = a_{22}\, a, \quad \alpha_2 = a_{22}\, \frac{b + \sqrt{\Delta}}{2}.$$

Hierin bedeute a_{22} die größte in $\mathfrak{m}$ aufgehende ganze rationale Zahl, $a_{22}\, a$ die kleinste durch $\mathfrak{m}$ teilbare ganze rationale Zahl; b ist eine Wurzel der Kongruenz:

$$b^2 \equiv \Delta \pmod{4\, a},$$

und es ist:

$$(2) \qquad \Delta = b^2 - 4\, a\, c.$$

$$(3) \qquad N(\mathfrak{m}) = a_{22}^2\, a.$$

Da $\mathfrak{m}$ relativ prim zu M vorausgesetzt ist, so können wir nach § 161, (6) in jeder in A vorkommenden Zahlklasse nach M eine durch $\mathfrak{m}$ teilbare Zahl α_0 bestimmen. Diese Zahl hat die Form

$$\alpha_0 = x_0\, \alpha_1 + y_0\, \alpha_2,$$

und wenn wir

$$(4) \qquad \begin{aligned} \alpha &= \alpha_0 + M\,(x\, \alpha_1 + y\, \alpha_2) \\ &= (x_0 + Mx)\, \alpha_1 + (y_0 + My)\, \alpha_2 \end{aligned}$$

setzen und x, y alle positiven und negativen ganzen rationalen Zahlen durchlaufen lassen, so durchläuft α die Gesamtheit der durch $\mathfrak{m}$ teilbaren und nach M mit α_0 kongruenten ganzen Zahlen der Gruppe A.

Um alle durch $\mathfrak{m}$ teilbaren ganzen Zahlen in A zu erhalten, haben wir ein vollständiges Restsystem nach M in Ω zu suchen und darunter die in A enthaltenen durch $\mathfrak{m}$ teilbaren Zahlen α_0 auszuwählen.

Soll die Norm dieser Zahl α nicht größer als t sein, so ergibt sich dafür, wenn wir die quadratische Form

$$a\, x^2 + b\, x\, y + c\, y^2$$

mit $\varphi(x, y)$ bezeichnen, die Bedingung:

$$\varphi\,(x_0 + Mx, \quad y_0 + My) \leqq \frac{t}{a_{22}^2\, a}, \qquad [\text{§ 91, (2), (4)}].$$

Nehmen wir in einer Ebene ein rechtwinkeliges Koordinatensystem X, Y an, und bezeichnen als Gitterpunkte die Punkte mit den Koordinaten

$$X = (x_0 + Mx)\, a_{22} \sqrt{\frac{a}{t}},$$

$$Y = (y_0 + My)\, a_{22} \sqrt{\frac{a}{t}},$$

worin x_0, y_0 festgehalten werden und x, y alle ganzen rationalen Zahlen durchläuft, so wird durch dieses Gitter die Ebene in Quadrate geteilt, deren Fläche

$$\delta^2 = M^2 \frac{a_{22}^2\, a}{t}$$

ist, und wenn T_0 die Anzahl der Gitterpunkte ist, die innerhalb der Ellipse

$$\varphi(X, Y) = 1$$

oder auf ihrer Grenze liegen, so ist $T_0\,\delta^2$ für ein unendliches t gleich dem Flächeninhalt dieser Ellipse, also gleich $\frac{\pi}{\sqrt{-\Delta}}$.

Berücksichtigt man noch die Flächenelemente δ^2, die von der Peripherie der Ellipse durchschnitten werden, aus denen man ein Maß für den Fehler dieser Flächenbestimmung erhält, so ist

$$(5) \qquad T_0 = \frac{\pi t}{M^2 a_{22}^2\, a \sqrt{-\Delta}} + R_0 \sqrt{t},$$

worin R_0 eine mit unendlich wachsendem t endlich bleibende Größe ist [Bd. II, § 194, (6)].

Einen solchen Ausdruck erhalten wir für jedes α_0, und wenn wir diese Ausdrücke alle addieren, so erhalten wir mit Rücksicht auf (3) den Satz:

Ist A eine Kongruenzgruppe mit dem Modul M und $\mathfrak{m}$ ein zu M teilerfremdes Ideal in Ω, ferner T die Anzahl der in $\overline{E}A$ enthaltenen ganzen Hauptideale, deren Norm nicht größer als t ist, so ist

$$(6) \qquad T = \frac{g\, t}{N(\mathfrak{m})} + R \sqrt{t},$$

worin g eine von $\mathfrak{m}$ und t unabhängige, von Null verschiedene Zahl und R eine mit unendlich wachsendem A endliche Funktion von t ist.

Die Konstante g ist nach (5) näher bestimmt:

$$(7) \qquad g = \frac{\gamma \pi}{M^2 \sqrt{-\Delta}},$$

wenn γ die Anzahl der in A enthaltenen Zahlklassen nach dem Modul M ist.

Will man unter T die Anzahl der ganzen Ideale der Hauptklasse $\bar{E}A$ verstehen, deren Norm nicht größer als t ist, so bleibt (6) auch dann noch bestehen, nur hat man, wenn -1 in A vorkommt, die Zahl g zu halbieren, und in den beiden Ausnahmefällen $\Delta = -4$, $\Delta = -3$ möglicherweise noch durch 4 oder durch 6 zu teilen.

§ 163. Die Dirichletschen Summen.

Wir verstehen jetzt unter $\bar{O}$ die Idealgruppe der sämtlichen Ideale in Ω (mit Rücksicht auf den Exkludenten S); A sei eine Kongruenzgruppe und

$$(1) \qquad \bar{A} = \bar{E}A,$$

die Gruppe der entsprechenden Hauptideale. Wir zerlegen $\bar{O}$ nach § 161, (3) in die Klassen nach A:

$$(2) \qquad \bar{O} = \bar{A}_1 + \bar{A}_2 + \cdots + \bar{A}_h,$$

und betrachten die Summen:

$$(3) \qquad S_i = \sum^{\mathfrak{a}_i} \frac{1}{(N\mathfrak{a}_i)^s},$$

worin s eine positive Variable > 1 bedeutet, und $\mathfrak{a}_i$ die sämtlichen ganzen Ideale einer Klasse $\bar{A}_i$ durchläuft.

Die Summen S_i formen wir in folgender Weise um:

Da $N(\mathfrak{a}_i)$ eine der Zahlen 1, 2, 3, ... sein muß, so bezeichnen wir mit a_ν die Anzahl der Ideale der Klasse $\bar{A}_i$, deren Norm $= \nu$ ist, und erhalten

$$(4) \qquad S_i = a_1 + \frac{a_2}{2^s} + \frac{a_3}{3^s} + \frac{a_4}{4^s} + \cdots$$

wobei, wenn eine Zahl ν unter der $N(\mathfrak{a}_i)$ nicht vorkommt, $a_\nu = 0$ zu setzen ist.

Bezeichnen wir mit $Z(\nu)$ die Anzahl der Ideale der Klasse $\bar{A}_i$, deren Norm nicht größer als ν ist, so erhalten wir für $Z(\nu)$ aus der Formel (6) des vorigen Paragraphen einen Grenzwert:

Wir nehmen nach § 161, 4. in der Klasse $(A_i)^{-1}$ ein zu M teilerfremdes Ideal $\mathfrak{m}$ und lassen in

(5) $$\mathfrak{m}\,\mathfrak{a}_i = \overline{\alpha}$$

$\mathfrak{a}_i$ die Ideale der Klasse $\overline{A}_i$, und folglich $\overline{\alpha}$ die durch $\mathfrak{m}$ teilbaren Ideale der Hauptklasse durchlaufen; ist dann

$$N(\mathfrak{a}_i) \overline{\gtrless}\, \nu,$$

so ist

$$N(\mathfrak{m})\, N(\mathfrak{a}_i) = N(\alpha) \overline{\gtrless}\, \nu\, N(\mathfrak{m}).$$

Bedeutet wie früher T die Anzahl der durch $\mathfrak{m}$ teilbaren Ideale der Hauptklasse, deren Norm nicht größer als t ist, so ist, wenn $t = \nu\, N(\mathfrak{m})$ gesetzt wird,

$$Z(\nu) = T,$$

und aus der Formel § 162, (6) ergibt sich

(6) $$Z(\nu) = g\,\nu + R_\nu \sqrt{\nu},$$

worin g eine Zahl, die für alle Klassen $\overline{A}_i$ dieselbe ist, und R_ν eine Funktion von ν bedeutet, die mit unendlich wachsendem ν nicht unendlich wird.

Nach der Bedeutung von a_ν ist

(7) $$a_\nu = Z(\nu) - Z(\nu - 1), \quad Z(0) = 0$$

und folglich

(8) $$S_i = \sum_{0,\infty}^{\nu} \frac{Z(\nu) - Z(\nu-1)}{\nu^s}.$$

Setzen wir für $Z(\nu)$ den Ausdruck (6), so folgt:

(9) $$S_i = g \sum \frac{1}{\nu^s} + \Sigma R_\nu \sqrt{\nu} \left(\frac{1}{\nu^s} - \frac{1}{(\nu+1)^s}\right).$$

Das zweite Glied dieser Summe:

$$\Sigma R_\nu \sqrt{\nu} \left(\frac{1}{\nu^s} - \frac{1}{(\nu+1)^s}\right)$$

ist unbedingt konvergent, solange $s > \frac{1}{2}$ ist, und ist daher eine stetige Funktion von s, die für $s = 1$ in

$$\sum_{1,\infty}^{\nu} \frac{R_\nu}{\sqrt{\nu}\,(\nu+1)}$$

übergeht; denn es ist

$$\lim_{\nu=\infty} \nu^{s+\frac{1}{2}} R_\nu \sqrt{\nu} \left(\frac{1}{\nu^s} - \frac{1}{(\nu+1)^s}\right) = s \operatorname{Lim} R_\nu$$

endlich. Die erste Summe in (9) ist

$$\sum \frac{1}{\nu^s} = \frac{1}{s-1} + C_s, \tag{10}$$

wo C_s für $s = 1$ endlich bleibt, nämlich in den Wert der Eulerschen Konstante 0,5772 ... übergeht (Bd. II, S. 723).

Berücksichtigt man dies, so ergibt sich aus (9) das Resultat:

5. Hat S_i die Bedeutung (3), so ist

$$S_i = \frac{g}{s-1} + C_i, \tag{11}$$

worin g eine von der besonderen Klasse $\bar{A}_i$ unabhängige von Null verschiedene Konstante ist, und C_i eine von $\bar{A}_i$ abhängige Funktion von s, die für $s = 1$ endlich bleibt.

Die Gruppe $h$ten Grades der Idealklasse $\bar{A}_i$ ist eine Abelsche, und es gibt daher h Charaktere $\chi_\varkappa(\bar{A}_i)$, die sämtlich $h$te Einheitswurzeln sind, darunter der Hauptcharakter χ_1, der für jede Klasse $= 1$ ist. Ebenso hat für die Hauptklasse $\bar{A}_1$ jeder der Charaktere den Wert $+1$. Für diese Charaktere bestehen die Sätze:

$$\begin{gathered} \sum^{i} \chi_\varkappa(\bar{A}_i) = 0, \quad \sum^{\varkappa} \chi_\varkappa(\bar{A}_i) = 0, \\ \varkappa = 2, 3, \ldots, h, \quad i = 2, 3, \ldots, h, \\ \sum^{i} \chi_1(\bar{A}_i) = h, \quad \sum^{\varkappa} \chi_\varkappa(\bar{A}_1) = h \end{gathered} \tag{12}$$

(Bd. II, § 13). Wenn das ganze Ideal $\mathfrak{a}$ in $\bar{O}$ in die Klasse $\bar{A}$ gehört, so setzen wir für jedes χ:

$$\chi(\mathfrak{a}) = \chi(\bar{A}), \tag{13}$$

und haben so für jedes Ideal in $\bar{O}$ die Charaktere nach der Gruppe A bestimmt. Für irgend zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ aus $\bar{O}$ besteht die Relation:

$$\chi(\mathfrak{a})\,\chi(\mathfrak{b}) = \chi(\mathfrak{a}\mathfrak{b}). \tag{14}$$

Nun bilden wir aus S_i die h Summe:

$$Q_\varkappa = \sum^{i} \chi_\varkappa(\bar{A}_i)\, S_i, \tag{15}$$

wofür wir nach (3) und (13) auch setzen können:

$$Q = \sum^{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{(N\mathfrak{a})^s}. \tag{16}$$

Darin kann χ jeder der Charaktere $\chi_\varkappa$ sein, und die Summe erstreckt sich über sämtliche Ideale $\mathfrak{a}$ von $\bar{O}$. Nach (11) ist, wenn wir

$$G_\varkappa = \sum^{i} \chi_\varkappa(\bar{A}_i)\, C_i$$

setzen,

$$(17) \qquad \begin{aligned} Q_1 &= \frac{h\,G}{s-1} + G_1, \\ Q_\varkappa &= \qquad\quad G_\varkappa, \quad \varkappa > 1. \end{aligned}$$

worin die $G_1, G_2, \ldots, G_h$ Funktionen von s sind, die für $s = 1$ einen endlichen Wert behalten.

Die Summen Q lassen sich in derselben Weise umformen, die wir schon im § 197 des zweiten Bandes kennen gelernt haben. Danach ist, wenn $\mathfrak{p}$ irgend ein Primideal in $\bar{O}$ bedeutet:

$$\begin{aligned} \frac{1}{1 - \chi(\mathfrak{p})\,N(\mathfrak{p})^{-s}} &= 1 + \chi(\mathfrak{p})\,N(\mathfrak{p})^{-s} + \chi(\mathfrak{p})^2\,N(\mathfrak{p})^{-2s} + \cdots \\ &= 1 + \frac{\chi(\mathfrak{p})}{N(\mathfrak{p})^s} + \frac{\chi(\mathfrak{p}^2)}{N(\mathfrak{p}^2)^s} + \frac{\chi(\mathfrak{p}^3)}{N(\mathfrak{p}^3)^s} + \cdots, \end{aligned}$$

und da sich alle Ideale $\mathfrak{a}$ als Produkte solcher Ideale $\mathfrak{p}$ darstellen lassen, so folgt:

$$(18) \qquad Q = \Pi \frac{1}{1 - \chi(\mathfrak{p})\,N(\mathfrak{p})^{-s}},$$

worin sich das unendliche Produkt Π auf alle Primideale $\mathfrak{p}$ in $\bar{O}$ erstreckt.

Zu jedem Ideal $\mathfrak{a}$ in $\bar{O}$ gehört ein gewisser Exponent φ, d. h. es gibt einen gewissen niedrigsten positiven Exponenten φ, für den $\mathfrak{a}^\varphi$ in der Hauptklasse $\bar{A}_1$ enthalten ist. Die Zahl φ ist immer ein Teiler der Klassenzahl h. Wir setzen:

$$(19) \qquad h = \varepsilon\,\varphi.$$

Gehört in diesem Sinne $\mathfrak{a}$ zum Exponenten φ, so sind sämtliche Charaktere $\chi_k(\mathfrak{a})$ φte Einheitswurzeln, und jede φte Einheitswurzel kommt darunter ε mal vor (Bd. II, § 198, 1.).

Gehört also $\mathfrak{p}$ zum Exponenten φ, so ist

$$\begin{aligned} \left[1 - \chi_1(\mathfrak{p})\,N(\mathfrak{p})^{-s}\right]\left[1 - \chi_2(\mathfrak{p})\,N(\mathfrak{p})^{-s}\right] \cdots \left[1 - \chi_h(\mathfrak{p})\,N(\mathfrak{p})^{-s}\right] \\ = \left[1 - N(\mathfrak{p})^{-\varphi s}\right]^\varepsilon, \end{aligned}$$

und es folgt aus (18):

$$(20) \qquad Q_1\,Q_2 \ldots Q_h = \Pi \frac{1}{\left[1 - N(\mathfrak{p})^{-\varphi s}\right]^\varepsilon}.$$

Es handelt sich nun um den Grenzwert, dem diese Ausdrücke sich nähern, wenn $s = 1$ wird.

Was die linke Seite betrifft, so folgt aus (17), daß

$$(21)\quad \begin{cases} \text{Lim}\,(s-1)\,Q_1 = h\,g \text{ endlich und von Null verschieden,} \\ \text{Lim}\, Q_2\, Q_3 \ldots Q_h \text{ endlich (vielleicht Null)} \end{cases}$$

ist. Zur Beurteilung der rechten Seite bemerken wir, daß die Primideale $\mathfrak{p}$ vom ersten oder vom zweiten Grade sind, und daß demnach $N(\mathfrak{p})$ gleich einer natürlichen Primzahl oder gleich dem Quadrat einer natürlichen Primzahl ist. Ferner stützen wir uns auf den bekannten Satz der Analysis, nach dem ein unendliches Produkt

$$(1-q_1)\,(1-q_2)\,(1-q_3)\ldots$$

unbedingt konvergiert und einen von Null verschiedenen Grenzwert hat, wenn

$$q_1 + q_2 + q_3 + \cdots$$

eine unbedingt konvergente Reihe ist, und keines der $q_i = 1$ ist.

Wir teilen danach die Primideale $\mathfrak{p}$ in zwei Arten, $\mathfrak{p}_1$, $\mathfrak{p}_2$, und zwar sollen die $\mathfrak{p}_1$ vom ersten Grade sein und zum Exponenten $\varphi = 1$ gehören (also $\varepsilon = h$). Die $\mathfrak{p}_2$ sollen entweder vom zweiten Grade sein, oder zu einem höheren Exponenten φ gehören. Es sind also $\mathfrak{p}_1$ die zur Hauptklasse $\bar{A}_1$ gehörigen Primideale ersten Grades.

Dann ist

$$N(\mathfrak{p}_1)^{\varphi} = N(\mathfrak{p}_1) = p_1$$

eine natürliche Primzahl und

$$N(\mathfrak{p}_2)^{\varphi} = p_2^k$$

mindestens die 2te (höchstens die $2h$te) Potenz einer Primzahl. Nach dem erwähnten analytischen Satze ist dann das Produkt

$$\Pi\,[1 - N(\mathfrak{p}_2)^{-s\varphi}]^{\varepsilon}$$

für $s = 1$ endlich und von Null verschieden, und es folgt aus (20), (21) der Satz:

6. Der Grenzwert

$$\text{Lim}_{s=1}\, \Pi\, \frac{s-1}{\Pi[1 - N(\mathfrak{p}_1)^{-s}]^h}$$

ist endlich, wenn $\mathfrak{p}_1$ die Primideale ersten Grades der Hauptklasse $\bar{A}_1$ durchläuft.

Ein besonderes Interesse nimmt die Frage in Anspruch, ob dieser Grenzwert verschwinden kann.

§ 164. Der Klassenkörper.

Zu der Zahlgruppe A in dem quadratischen Körper Ω soll ein algebraischer Körper über Ω existieren, den man mit $\mathfrak{K}$ oder $\mathfrak{K}(A)$ bezeichne, von dem wir nur voraussetzen wollen:

7. Definition des Klassenkörpers.

Die Primideale $\mathfrak{p}_1$ ersten Grades der Hauptklasse $\bar{A}_1$, und nur diese, sollen im Körper $\mathfrak{K}(A)$ wieder in Primideale ersten Grades zerfallen.

Es sind also nur die Primideale in Ω, die wir vorhin mit $\mathfrak{p}_1$ bezeichnet haben, die in $\mathfrak{K}$ in Primideale ersten Grades zerfallen.

Eine beliebige endliche Anzahl von Primzahlen können dabei ausgenommen sein. Sie werden dann in den Exkludenten genommen.

Ist n der relative Grad des Körpers $\mathfrak{K}$ über Ω und p eine natürliche Primzahl, in der die Ideale $\mathfrak{p}_1$ und $\mathfrak{P}$ in Ω und $\mathfrak{K}$ aufgehen, und bezeichnet man mit N_Ω, $N_\mathfrak{K}$ die absoluten Normen im Körper Ω und $\mathfrak{K}$, so ist

$$N_\mathfrak{K}(\mathfrak{P}) = N_\Omega(\mathfrak{p}_1) = p, \quad N_\mathfrak{K}(\mathfrak{p}_1) = p^n,$$

und folglich muß $\mathfrak{p}_1$ im Körper $\mathfrak{K}$ in n Primideale $\mathfrak{P}$ zerfallen:

(1) $$\mathfrak{p}_1 = \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_n.$$

Die Primideale, die in den Grundzahlen der Körper Ω oder $\mathfrak{K}$ aufgehen, sollen immer ausgeschlossen sein. Dann sind die $\mathfrak{P}_1$, $\mathfrak{P}_2, \ldots, \mathfrak{P}_n$ voneinander verschieden.

Ob ein solcher Körper $\mathfrak{K}$ existiert, bleibt vorläufig unentschieden. Wir wollen untersuchen, was aus der Definition geschlossen werden kann.

Da in jedem Ideal $\mathfrak{p}_1$ n Ideale $\mathfrak{P}$ aufgehen, so ist

(2) $$\Pi\left[1 - N_\mathfrak{K}(\mathfrak{p}_1)^{-s}\right]^n = \Pi\left[1 - N_\mathfrak{K}(\mathfrak{P})^{-s}\right],$$

worin sich das erste Produkt auf alle Ideale $\mathfrak{p}_1$ des Körpers Ω, das zweite auf alle Ideale $\mathfrak{P}$ ersten Grades des Körpers $\mathfrak{K}$ erstreckt, und nach dem für jeden beliebigen Körper gültigen Satz I, § 197 des II. Bandes hat

(3) $$(s-1)\,\Pi \frac{1}{\left[1 - N_\mathfrak{K}(\mathfrak{P})^{-s}\right]}$$

für $s = 1$ einen von Null verschiedenen endlichen Grenzwert, der dort auf die Klassenzahl im Körper $\mathfrak{K}$ zurückgeführt ist. Setzen wir zur Abkürzung

(4) $$P = \Pi \frac{1}{[1 - N(\mathfrak{p}_1)^{-s}]},$$

so ist nach (2) und (3) für $s = 1$

(5) $(s - 1) P^n$ endlich und von Null verschieden,

und nach § 163, 6.:

(6) $(s - 1) P^h$ endlich,

und wenn man hieraus P eliminiert, so folgt:

$$(s - 1)^{n-h} \text{ endlich.}$$

Also ist

(7) $$n \geqq h.$$

Daraus folgt der Satz:

8. Der Relativgrad n des Klassenkörpers kann nicht kleiner sein als die Klassenzahl h der Gruppe. Ist $n = h$, so ist $(s - 1) P^h$ für $s = 1$ nicht Null, und die Summen $Q_2, Q_3, \ldots, Q_h$ sind gleichfalls von Null verschieden.

Kann man eine Gleichung in Ω vom Grade h bilden, aus der sich ein Körper ableiten läßt, der die charakteristischen Eigenschaften des Klassenkörpers erkennen läßt, und ist der Grad dieses Körpers nicht größer als h, so folgt also, daß er auch nicht kleiner sein kann, also $= h$ sein muß. Damit ist die Irreduzibilität der fraglichen Gleichung erwiesen.

Hierauf beruht der Nachweis der Irreduzibilität der Kreisteilungsgleichung, den wir im § 198 des II. Bandes gegeben haben. Dort trat an Stelle von Ω der Körper der rationalen Zahlen. Im nächsten Abschnitt werden wir noch weitere Anwendungen hiervon machen.

Ob es Gruppen gibt, bei denen der Grad des Klassenkörpers größer als die Klassenzahl ist, bleibt dahingestellt. Ich halte es für unwahrscheinlich.

Wir beweisen noch, daß es höchstens einen Klassenkörper geben kann. Jeder solche Körper wird durch Adjunktion einer algebraischen Zahl ξ zu Ω erzeugt.

Es sei ξ eine den Klassenkörper $\mathfrak{K} = \Omega(\xi)$ erzeugende ganze Zahl, die also einer in Ω irreduzibelen Gleichung

(8) $$f(\xi) = \xi^n + \alpha_1 \xi^{n-1} + \alpha_2 \xi^{n-2} + \cdots + \alpha_n = 0$$

genügt, in der die $\alpha_1, \alpha_2, \ldots, \alpha_n$ ganze Zahlen in Ω sind.

Jede ganze Zahl η des Körpers $\mathfrak{K}$ kann (Bd. I, § 151) in der Form dargestellt werden:

$$\eta = \frac{\varphi(\xi)}{f'(\xi)},$$

worin $\varphi(\xi)$ ganze Koeffizienten in Ω hat. Man kann dies in die Form setzen:

$$(9) \qquad \gamma\eta = \gamma_0 + \gamma_1\xi + \gamma_2\xi^2 + \cdots + \gamma_{n-1}\xi^{n-1},$$

worin $\gamma, \gamma_0, \gamma_1, \ldots, \gamma_{n-1}$ ganze Zahlen in Ω sind, und so, daß die erste, γ, ein Teiler der Diskriminante von f ist. Die Primfaktoren von γ schließen wir durch den Exkludenten aus.

Es sei

$\mathfrak{P}$ ein Primideal ersten Grades in $\mathfrak{K}$,

$\mathfrak{p}_1$ das durch $\mathfrak{P}$ teilbare Primideal ersten Grades in Ω,

p die Norm von $\mathfrak{p}_1$ und von $\mathfrak{P}$;

dann ist für jede ganze Zahl α in Ω:

$$\alpha^p \equiv \alpha \pmod{\mathfrak{p}_1}$$

und

$$(10) \qquad \xi^p \equiv \xi \pmod{\mathfrak{P}},$$

also nach (9) für jede ganze Zahl η in $\mathfrak{K}$:

$$\eta^p \equiv \eta \pmod{\mathfrak{P}}.$$

9. Die notwendige und hinreichende Bedingung dafür, daß $\mathfrak{K}(\xi)$ Klassenkörper sei, besteht also darin, daß für jedes in einem $\mathfrak{p}_1$ aufgehende Primideal $\mathfrak{P}$ und nur für dieses die Kongruenz (10) erfüllt sei.

Es seien nun

$$\mathfrak{K} = \Omega(\xi), \quad \mathfrak{K}' = \Omega(\xi')$$

zwei Klassenkörper derselben Gruppe A. Zunächst ergibt sich leicht, daß sie von gleichem Grade sein müssen. Denn für beide muß die Bedingung (5) erfüllt sein. Sind also n und n' die Grade, so muß $(s - 1)^{n'-n}$ für $s = 1$ endlich und von Null verschieden sein, was nur möglich ist, wenn $n = n'$ ist.

Durch Zusammensetzung von $\mathfrak{K}$ und $\mathfrak{K}'$ leiten wir einen dritten Körper ab:

$$\mathfrak{K}'' = \Omega(\xi, \xi'),$$

von dem wir zeigen, daß er auch ein Klassenkörper ist.

Den Körper $\mathfrak{K}''$ können wir erzeugen durch eine Zahl:

(11) $$\xi'' = \alpha\xi + \alpha'\xi',$$

in der α, α' ganze Zahlen in Ω sind.

Es sei $\mathfrak{P}''$ ein in einem $\mathfrak{p}_1$ aufgehendes Primideal in $\mathfrak{K}''$ und $\mathfrak{P}, \mathfrak{P}'$ die durch $\mathfrak{P}''$ teilbaren Primideale in $\mathfrak{K}, \mathfrak{K}'$ und $N(\mathfrak{p}_1) = p$. Dann ist nach 9.:

(12) $$\xi^p \equiv \xi \pmod{\mathfrak{P}}, \quad \xi'^p \equiv \xi' \pmod{\mathfrak{P}'},$$

und folglich ist nach (11):

(13) $$\xi''^p \equiv \alpha^p \xi^p + \alpha'^p \xi'^p \equiv \xi'' \pmod{\mathfrak{P}''}.$$

Ist umgekehrt die Kongruenz (13) befriedigt, so folgen daraus wieder die Kongruenzen (12), weil man ξ und ξ' rational [in der Form (9)] durch ξ'' ausdrücken kann.

Es ist also $\mathfrak{K}''$ ebenfalls Klassenkörper, und sein Grad ist ebenso hoch wie der von $\mathfrak{K}$ und $\mathfrak{K}'$. Es sind also ξ und ξ' primitive Zahlen von $\mathfrak{K}''$, und folglich sind alle diese Körper identisch (Bd. I, § 151, 3.). Ist $\mathfrak{K}$ ein Klassenkörper, so sind die mit $\mathfrak{K}$ konjugierten Körper auch Klassenkörper und sind daher mit $\mathfrak{K}$ identisch.

Damit ist der Satz bewiesen:

10. Es gibt für eine gegebene Zahlgruppe nur einen Klassenkörper, und dies ist ein Normalkörper.

Wir wollen nun die hauptsächlichsten Eigenschaften und Anwendungen des Klassenkörpers in den aus der komplexen Multiplikation stammenden Fällen näher kennen lernen.

Nehmen wir an, daß die Zahlgruppe A eine andere Gruppe A' als Teiler von endlichem Index $(A; A')$ enthalte, und daß diese beiden Gruppen Klassenkörper besitzen:

(14) $$\mathfrak{K} = \mathfrak{K}(A) = \Omega(\xi), \quad \mathfrak{K}' = \mathfrak{K}(A') = \Omega(\xi'),$$

dann läßt sich beweisen, daß der Körper $\mathfrak{K}$ in $\mathfrak{K}'$ enthalten ist. Sind nämlich $\mathfrak{p}_1$, $\mathfrak{p}_1'$ die Primideale in Ω ersten Grades der Hauptklassen $\bar{A}_1$, $\bar{A}_1'$, dann sind die $\mathfrak{p}_1'$ unter den $\mathfrak{p}_1$ enthalten. Wenn daher p die Primzahl ist, in der $\mathfrak{p}_1$ und $\mathfrak{p}_1'$ aufgeht, so ist nach 9.:

(15) $$\xi^p \equiv \xi \pmod{\mathfrak{P}} \text{ für alle } \mathfrak{p}_1 \text{ und folglich für alle } \mathfrak{p}_1', \quad \xi'^p \equiv \xi' \pmod{\mathfrak{P}'} \text{ für alle } \mathfrak{p}_1',$$

wenn $\mathfrak{P}$ und $\mathfrak{P}'$ Primideale ersten Grades in $\mathfrak{K}$ und $\mathfrak{K}'$ sind.

Wir bilden jetzt den Körper:

(16) $$\mathfrak{K}'' = \Omega(\xi, \xi') = \Omega(\xi''),$$

indem wir

(17) $$\xi'' = \alpha\xi + \alpha'\xi'$$

setzen, und bezeichnen ein Primideal ersten Grades dieses Körpers, das in einem $\mathfrak{p}_1'$ aufgeht, mit $\mathfrak{P}''$.

$\mathfrak{P}$, $\mathfrak{P}'$ seien, wie oben, die durch $\mathfrak{P}''$ teilbaren Primideale in $\mathfrak{K}$, $\mathfrak{K}'$. Dann ist nach (15) und (17)

$$\xi''^{p} \equiv \xi'' \pmod{\mathfrak{P}''},$$

und folglich ist $\mathfrak{K}''$ ein Klassenkörper von A'.

Demnach ist $\mathfrak{K}''$ mit $\mathfrak{K}'$ identisch; ξ' ist eine primitive Zahl von $\mathfrak{K}''$, und folglich kann jede Zahl in $\mathfrak{K}''$, also auch ξ, rational durch ξ' ausgedrückt werden.

Daraus folgt:

11. Enthält eine Zahlgruppe A eine andere Zahlgruppe A' als Teiler von endlichem Index, und existieren die Klassenkörper $\mathfrak{K}(A)$, $\mathfrak{K}(A')$, so ist $\mathfrak{K}(A)$ in $\mathfrak{K}(A')$ enthalten.

§ 165. Primideale in den Klassen.

Wir kehren jetzt zu den Funktionen Q zurück, die wir in § 163, (16) durch unendliche Reihen und in § 163, (18) durch unendliche Produkte:

(1) $$Q_\varkappa = \Pi \frac{1}{1 - \chi_\varkappa(\mathfrak{p})\, N(\mathfrak{p})^{-s}}$$

dargestellt haben, worin $\chi_\varkappa$ einen der Charaktere der Gruppe bedeutet und $\mathfrak{p}$ alle Primideale in $\overline{O}$ durchläuft. Den Logarithmus dieses Produktes entwickeln wir in folgender Weise:

(2) $$\log Q_\varkappa = \sum \frac{\chi_\varkappa(\mathfrak{p})}{N(\mathfrak{p})^s} + \frac{1}{2}\sum \frac{\chi_\varkappa(\mathfrak{p}^2)}{N(\mathfrak{p})^{2s}} + \frac{1}{3}\sum \frac{\chi_\varkappa(\mathfrak{p}^3)}{N(\mathfrak{p})^{3s}} + \cdots$$

Das Vielfache von $2\pi i$, das in dem $\log Q$ nicht näher definiert ist, brauchen wir nicht zu kennen, da es sich mit s nur unstetig ändern könnte, und da rechts und links stetige Funktionen von s stehen, solange $s > 1$ ist, so ändert sich dieses Vielfache überhaupt nicht mit s.

Es sei $\overline{A}_i$ eine der Klassen der Idealgruppe $\overline{A}$ und $\overline{A}_i'$ die entgegengesetzte Klasse. Dann ist nach (12), (13), (14), § 163:

$$\sum^{h} \chi_\varkappa(\overline{A}_i')\, \chi_\varkappa(\mathfrak{a}) = h \text{ oder } = 0,$$

je nachdem das Ideal $\mathfrak{a}$ in der Klasse A_i oder in einer anderen Klasse enthalten ist. Multiplizieren wir also die Formel (2) mit $\chi_\varkappa(\bar{A}'_i)$ und summieren in bezug auf $\varkappa$, so folgt:

$$(3) \qquad \begin{aligned} &\frac{1}{h}\overset{\varkappa}{\Sigma}\,\chi_\varkappa(A'_i)\log Q_k \\ &= \overset{(1)}{\sum}\frac{1}{N(\mathfrak{p})^s} + \frac{1}{2}\overset{(2)}{\sum}\frac{1}{N(\mathfrak{p})^{2s}} + \frac{1}{3}\overset{(3)}{\sum}\frac{1}{N(\mathfrak{p})^{3s}} + \cdots, \end{aligned}$$

worin sich die Summen $\overset{(1)}{\Sigma}, \overset{(2)}{\Sigma}, \overset{(3)}{\Sigma}, \ldots$ auf alle Primideale $\mathfrak{p}$ erstrecken, deren erste, zweite, dritte, ... Potenz in der Klasse $\bar{A}_i$ enthalten ist.

Wir gehen in (3) zur Grenze $s = 1$ über; die Summen $\overset{(2)}{\Sigma}, \overset{(3)}{\Sigma}, \ldots$ behalten dabei einen endlichen Wert, da ihre unbedingte Konvergenz für $s = 1$ nicht aufhört. Dasselbe gilt von dem Teil der Summe $\overset{(1)}{\Sigma}$, der sich auf Primideale von höherem als dem ersten Grade bezieht, und es bleibt also nur noch fraglich, ob die Summe

$$\sum\frac{1}{N(\mathfrak{p})^s},$$

erstreckt über alle Primideale ersten Grades der Klasse $\bar{A}_i$, endlich bleibt oder unendlich wird. Ersteres würde der Fall sein, wenn es in $\bar{A}_i$ gar keine oder nur eine endliche Anzahl von Primidealen ersten Grades gäbe.

Setzen wir aber die Existenz eines Klassenkörpers vom Grade h voraus, so folgt aus § 164, 8. und § 163, (21), daß

$$\log Q_2,\ \log Q_3, \ldots, \log Q_h$$

endliche Grenzwerte behalten, während $\log Q_1$ unendlich wird. Die linke Seite von (3) wird also unendlich und die rechte Seite kann nicht endlich bleiben.

Damit ist bewiesen:

12. Wenn ein Klassenkörper existiert, dessen Grad nicht höher ist als die Klassenzahl, so enthält jede Klasse unendlich viele Primideale ersten Grades.

§ 166. Primideale in den Idealklassen.

Nehmen wir als Gruppe zunächst die Gesamtheit der Zahlen O des Körpers Ω ohne die Null, so sind die Klassen die Idealklassen des Körpers Ω, die, wie wir gesehen haben, den Klassen quadratischer Formen der Diskriminante Δ eindeutig zugeordnet

werden können. Nehmen wir als Gruppe die Ordnung $O' = [Q]$ mit dem Führer Q, die durch die Kongruenzbedingung definiert ist, daß jede Zahl in O' nach dem Modul Q mit einer rationalen Zahl kongruent sein soll, so haben wir eine Kongruenzgruppe, deren Exkludent und Modul $= Q$ ist. Die Klassen entsprechen den Formenklassen der Diskriminante $D = Q^2 \varDelta$. Der zweite Fall schließt den ersten in sich (für $Q = 1$). Der Klassenkörper ist hier der Klassenkörper $\mathfrak{K}(D)$, den wir zum Unterschied von allgemeineren als Ordnungskörper bezeichnen wollen.

Denn ist (k) eine Klasseninvariante, so ist (§ 122)

$$(k)^p \equiv (k) \pmod{\mathfrak{P}}$$

nur dann befriedigt, wenn p durch die Hauptklasse der Diskriminante D darstellbar ist. Dann zerfällt p in Ω in zwei konjugierte Primideale $\mathfrak{p}$, $\mathfrak{p}'$, die durch Zahlen in O oder in O' darstellbar, also Hauptideale sind.

Der Körper $\mathfrak{K}(\varDelta)$ ist der Klassenkörper von Ω im engeren Sinne, der den Idealklassen dieses Körpers entspricht, und auch als Haupt-Klassenkörper $\mathfrak{K}(\Omega)$ bezeichnet sein mag.

In jeder Idealklasse, sowohl nach O als nach O', gibt es also unendlich viele Primideale ersten Grades. Mit anderen Worten: Ist $\mathfrak{a}$ ein beliebiges (zu Q teilerfremdes) Ideal, so gibt es unendlich viele Primideale $\mathfrak{p}$, die mit $\mathfrak{a}$ nach O' äquivalent sind. Dann sind nach § 95 auch die den Idealen $\mathfrak{a}$ und $\mathfrak{p}$ entsprechenden Formen äquivalent, und p ist durch die zu $\mathfrak{a}$ gehörige Form darstellbar. Damit ist der Satz bewiesen:

1. Durch jede primitive Form der Diskriminante D sind unendlich viele Primzahlen darstellbar[1]).

§ 167. Primzahlen in Linearformen.

Wir definieren nun eine Zahlgruppe A in Ω folgendermaßen:

[1]) Dieser Satz, sowohl für negative als für positive Diskriminanten, ist zuerst von Dirichlet bewiesen, der Beweis aber nur in einem speziellen Fall publiziert (Bericht der Berliner Akademie 1840, Werke Bd. I, S. 497). Der ausgeführte Beweis ist von H. Weber gegeben (Mathematische Annalen XX, 1882). Eine gleichfalls von Dirichlet herrührende Verallgemeinerung, auf die wir im nächsten Paragraphen zurückkommen, ist von A. Meyer bewiesen (Crelles Journ., Bd. 103). Der hier im Text gegebene Beweis beruht auf anderer Grundlage, bezieht sich aber freilich einstweilen (solange der Klassenkörper für positive Diskriminanten nicht bekannt ist) nur auf negative Diskriminanten.

Es sei $\mathfrak{m}$ ein ganzes Ideal in Ω, und A bestehe aus allen ganzen und gebrochenen Zahlen α in Ω, die zu $\mathfrak{m}$ teilerfremd sind und der Bedingung genügen:

$$\alpha \equiv 1 \pmod{\mathfrak{m}}. \tag{1}$$

Nehmen wir die Primteiler von $\mathfrak{m}$ in den Exkludenten, und bezeichnen mit O die Gruppe der Zahlen in Ω, so zerfällt O nach dem Modul $\mathfrak{m}$ in $\psi(\mathfrak{m})$ Zahlklassen, worin $\psi(\mathfrak{m})$ die Bedeutung wie in Bd. II, § 168 hat, nämlich, wenn $\mathfrak{p}$ die Primteiler von $\mathfrak{m}$ durchläuft:

$$\psi(\mathfrak{m}) = N(\mathfrak{m})\, \Pi\left(1 - \frac{1}{N(\mathfrak{p})}\right). \tag{2}$$

In die Gruppe A gehören nicht bloß einzelne Zahlen, sondern Zahlklassen nach dem Modul $\mathfrak{m}$. Hiernach ist:

$$(O, A) = \psi(\mathfrak{m}). \tag{3}$$

Um die Klassenzahl für unsere Gruppe zu bestimmen, wenden wir die Sätze des § 161 an.

Danach ist, wenn $\bar{E}$ die Gruppe der funktionalen Einheiten und E die Gruppe der numerischen Einheiten bedeutet:

$$(\bar{O}, \bar{E}A) = (\bar{O}, \bar{E}O)\,(\bar{E}O, \bar{E}A),$$
$$(\bar{E}O, \bar{E}A) = (\bar{E}O, \bar{E}EA) = (O, EA).$$

Weiter ist

$$(O, EA)\,(EA, A) = (O, A) = \psi(\mathfrak{m}).$$

$(EA, A) = e$ ist die Zahl der nach $\mathfrak{m}$ inkongruenten Einheiten, und

$$(\bar{O}, \bar{E}O) = H$$

die Klassenzahl des Körpers Ω,

$$(\bar{O}, \bar{E}A) = h$$

die Klassenzahl nach A. Daraus ergibt sich:

$$h = \frac{H\,\psi(\mathfrak{m})}{e}. \tag{4}$$

Die Zahl e ist im allgemeinen gleich der Anzahl der Einheiten in Ω, also $= 2$, und in den beiden Ausnahmefällen $\Delta = -4$, $\Delta = -3$ ist $e = 4$ und $e = 6$. Die Zahl e ist kleiner, wenn unter den Einheiten Kongruente (modulo $\mathfrak{m}$) vorkommen, was nur möglich ist, wenn $\mathfrak{m}$ ein Teiler von 2 oder von 3 ist.

Bedeutet E die Gruppe der Einheiten oder auch eine darin enthaltene Gruppe, so bekommen wir denselben Wert der Klassenzahl und denselben Klassenkörper, wenn wir EA an Stelle von A treten lassen.

Dies gilt nicht nur für diese besondere Gruppe, sondern allgemein. Wir hätten also z. B. die Zahlen α der Gruppe A auch durch

$$\alpha \equiv \pm 1 \pmod{\mathfrak{m}}$$

definieren können, denn $E = +1, -1$ ist auch in den Ausnahmefällen $\Delta = -4$, $\Delta = -3$ eine Gruppe.

Nun läßt sich nachweisen, daß der Teilungskörper $\mathfrak{T}_{\mathfrak{m}}$ der Klassenkörper zu A ist. Schließen wir zunächst noch alle in der Diskriminante des Teilungskörpers aufgehenden Primfaktoren aus, und bezeichnen mit τ irgend eine Zahl des Teilungskörpers, so ist nach § 160

$$\tau^p \equiv \tau \pmod{\mathfrak{p}} \tag{5}$$

nur dann erfüllt, wenn $\mathfrak{p}$ ein Primideal ersten Grades in Ω ist, das der Hauptklasse angehört. Das aber ist das Kennzeichen des Klassenkörpers. Der Grad des Teilungskörpers ist aber nach § 154 höchstens gleich dem in (4) gegebenen Ausdruck h, folglich ist er genau gleich h und die Teilungsgleichung irreduzibel. Außerdem ist damit bewiesen, daß es in jeder der Idealklassen $\overline{A}_\nu$ nach A unendlich viele Primideale ersten Grades gibt.

Man kann diesem Satz folgenden Ausdruck geben:

Ist β eine beliebige Zahl in O, $\mathfrak{a}$ ein beliebiges Ideal in $\overline{O}$, so ist durch

$$\overline{A}_\nu = \mathfrak{a}\beta A \tag{6}$$

eine Klasse nach A bestimmt (§ 161), und in dieser Klasse sind unendlich viele Primideale ersten Grades enthalten. Ein solches Primideal ist nach (6) in der Form darstellbar:

$$\mathfrak{p} = \mathfrak{a}\beta\alpha, \tag{7}$$

worin $\alpha \equiv 1 \pmod{\mathfrak{m}}$ ist. Setzen wir also

$$\alpha\beta = \pi,$$

so ist

$$\pi \equiv \beta \pmod{\mathfrak{m}}.$$

Daraus folgt:

2. Ist β eine Zahl in O, $\mathfrak{a}$ ein Ideal in $\overline{O}$, so gibt es unendlich viele im allgemeinen gebrochene Zahlen π in O, die der Bedingung

(8) $$\pi \equiv \beta \pmod{\mathfrak{m}}$$

genügen, für die

(9) $$\mathfrak{p} = \mathfrak{a}\pi$$

ein Primideal wird.

Nimmt man $\mathfrak{a} = 1$, so wird π eine ganze Zahl, also eine in Ω existierende Primzahl. Der Satz lautet für diesen besonderen Fall:

3. Es gibt im Körper Ω unendlich viele existierende Primzahlen π, deren Norm eine natürliche Primzahl ist, die nach einem beliebigen Modul $\mathfrak{m}$ mit einer beliebigen zu $\mathfrak{m}$ teilerfremden Zahl β kongruent sind.

Nehmen wir für den Modul $\mathfrak{m}$ eine ganze Zahl μ in Ω, so erhalten wir folgenden Satz:

4. Ist μ eine ganze Zahl in Ω, so sind in der Linearform

$$\mu\xi + \beta,$$

in der ξ die ganzen Zahlen von Ω durchläuft und β relativ prim zu μ ist, unendlich viele Primzahlen enthalten.

Man hat hier eine schöne Verallgemeinerung des Satzes von den Primzahlen in arithmetischen Progressionen (Bd. II, § 198)[1].

§ 168. Reduktion der Klassengleichung in den Kreisteilungskörpern.

Wir definieren eine weitere Gruppe A durch folgende Bestimmung:

Es seien Q, m zwei ganze rationale Zahlen, deren Primfaktoren wir in den Exkludenten S aufnehmen. O sei wie in § 98 die Gruppe der Zahlen in Ω, und O' die Gruppe der Zahlen der Ordnung $[Q]$, und A bestehe aus allen ganzen und gebrochenen Zahlen α in O', die der Kongruenzbedingung

(1) $$N(\alpha) \equiv 1 \pmod{m}$$

genügen. Zunächst haben wir die Klassenzahl

(2) $$h = (\bar{O}, \bar{E}A) = (\bar{O}, \bar{E}O')(\bar{E}O', \bar{E}A)$$

[1]) Für den Fall $\Delta = -4$ ist dieser Beweis gegeben von H. Weber, Crelles Journ., Bd. 129 (Dirichlet-Band), für $\Delta = -3$ in einer Straßburger Dissertation von H. Bresslau (Straßburg 1907).

zu bestimmen. Der erste Faktor ist die Klassenzahl der quadratischen Formen der Ordnung O' [§ 100, (3)], die wir mit H' bezeichnen. Es ist also

$$(3) \qquad h = H'(\bar{E}O', \bar{E}A) = H'(O', A)$$

(nach § 100, 13.).

Es bleibt noch (O', A) zu bestimmen.

Bedeutet $\varrho_1, \varrho_2, \ldots, \varrho_\mu$ ein vollständiges Repräsentantensystem von O' nach A, so müssen die Zahlen

$$(4) \qquad N(\varrho_1), N(\varrho_2) \ldots, N(\varrho_\mu)$$

nach dem Modul m alle verschieden sein, und jede Norm einer Zahl in O ist mit einer dieser Zahlen nach m kongruent. Ist daher Z die Gruppe der rationalen Zahlen, M die Gruppe der Zahlen z aus Z, die der Bedingung

$$z \equiv 1 \pmod{m}$$

genügen, R_m die Gruppe der Normenreste nach m, so ist (4) ein vollständiges Repräsentantensystem von R_m nach M und folglich

$$\mu = (O', A) = (R_m, M).$$

Dafür kann man auch setzen (§ 100, 12.):

$$(5) \qquad (O', A) = \frac{(Z, M)}{(Z, R_m)}.$$

Nun ist

$$(6) \qquad (Z, M) = \varphi(m) = m\Pi\left(1 - \frac{1}{r}\right),$$

wenn r die Primfaktoren von m durchläuft und folglich

$$(7) \qquad h = \frac{H'\varphi(m)}{(Z, R_m)}.$$

Den Klassenkörper $\mathfrak{K}(A)$ unserer Gruppe erhalten wir, wenn wir dem Klassenkörper $\mathfrak{K}(D)$ eine primitive $m$te Einheitswurzel adjungieren:

$$(8) \qquad \mathfrak{K}(A) = \mathfrak{K}(D, \varrho).$$

Denn die Bedingung dafür, daß ein in einer Primzahl p aufgehendes Primideal $\mathfrak{P}$ des Körpers $\mathfrak{K}(D, \varrho)$ vom ersten Grade sei, ist, wenn (k) eine Klasseninvariante der Diskriminante D bedeutet:

$$(9) \qquad (k)^p \equiv (k), \quad \varrho^p \equiv \varrho \pmod{\mathfrak{P}},$$

wenn alle störenden Primzahlen, z. B. die in den Diskriminanten der die Zahlen (k) und (ϱ) definierenden Gleichungen, in den Exkludenten S aufgenommen sind.

Die erste der Bedingungen (9) fordert, daß p durch die Hauptform der Diskriminante D eigentlich darstellbar sei (§ 122), die zweite, daß

$$p \equiv 1 \pmod{m} \tag{10}$$

sei.

Damit ein Primideal $\mathfrak{p}$ ersten Grades in Ω, das nicht in S aufgeht, in $\bar{E}A$ enthalten sei, ist notwendig und hinreichend, daß

1. $\mathfrak{p}$ ein Hauptideal, d. h. eine existierende Zahl π sei, und daß diese Zahl π in A enthalten sei, d. h. daß

2. $N(\pi) = p \equiv 1 \pmod{m}$

sei. Diese Bedingungen stimmen genau mit den Bedingungen (9) überein, und folglich ist $\mathfrak{K}(D, \varrho)$ der Klassenkörper der Gruppe A.

Der Grad des Körpers $\mathfrak{K}(A)$ ist daher nicht nur höchstens, sondern genau gleich h.

Die Zahl (Z, R_m) ist $= 1$, wenn in m keine der charakteristischen Primzahlen des § 108 aufgeht, und dann ist der Grad des Körpers $\mathfrak{K}(A)$ gleich $H' \varphi(m)$. Nehmen wir umgekehrt alle charakteristischen Primzahlen und Primzahlpotenzen in m auf, so wird $R_m = R$ die Gruppe der absoluten Normenreste, und es ist

$$(Z, R) = 2g,$$

wenn g die Anzahl der Geschlechter der Diskriminante D ist (§ 113, 7.). Bezeichnet also H'_g die Anzahl der Klassen eines Geschlechtes, so ist $H' = g H'_g$, und die Formel (7) ergibt:

$$h = \tfrac{1}{2} H'_g \varphi(m). \tag{11}$$

Nach § 138 zerfällt die Klassenfunktion $H_{-D}(u)$ durch Adjunktion von Quadratwurzeln in so viele Faktoren, als es Geschlechter von Formenklassen gibt, und der Grad eines jeden dieser Faktoren ist H'_g.

Wäre nun die Klassengleichung durch Adjunktion irgend welcher Einheitswurzeln noch weiter zerlegbar, als nach den Geschlechtern, so könnte man m so annehmen, daß auch diese Einheitswurzeln und auch $\sqrt{\Delta}$ in dem Körper $\mathfrak{R}(\varrho)$ enthalten wären.

Ist dann h'' der niedrigste Grad, auf den die Klassengleichung durch Adjunktion von Einheitswurzeln reduziert werden kann, so ist der absolute Grad des Körpers $\mathfrak{K}(D, \varrho)$ höchstens gleich $h'' \varphi(m)$

und der Relativgrad in bezug auf Ω höchstens gleich $\frac{1}{2}h''\varphi(m)$, und daraus geht nach (11) hervor, daß h'' nicht kleiner als H'_g sein kann. Damit ist bewiesen:

5. Die Klassengleichung $H_{-D}(u)$ ist in dem Körper, der alle Einheitswurzeln enthält, nicht weiter zerlegbar als in die den Geschlechtern entsprechenden Faktoren.

§ 169. Beziehung der Teilungskörper zu dem Klassenkörper.

Wir haben in den beiden letzten Paragraphen zwei Arten von Gruppen betrachtet, von denen die erste zu den Teilungskörpern der elliptischen Funktionen, die zweite zu den Ordnungskörpern in Verbindung mit Einheitswurzeln führte. Zwischen diesen besteht eine Beziehung:

Die erste Gruppe A bestand aus den Zahlen α in O, die der Bedingung

(1) $$\alpha \equiv \pm 1 \pmod{\mathfrak{m}}$$

genügten, wenn $\mathfrak{m}$ irgend ein Ideal in Ω ist, die zweite Gruppe A' bestand aus den Zahlen α' der Ordnung $[Q]$, die der Bedingung

(2) $$N(\alpha') \equiv 1 \pmod{m}$$

genügten, wenn m und Q natürliche Zahlen bedeuten.

Nehmen wir an, es sei $\mathfrak{m}$ ein Primideal oder eine Potenz eines Primideals, so können wir Q und m so annehmen, daß die Gruppe A' in der Gruppe A enthalten ist.

Denn ist r eine rationale Zahl, so ist, da α' der Ordnung $[Q]$ angehört:

(3) $$\alpha' \equiv r \pmod{Q}, \quad N(\alpha') \equiv r^2 \pmod{Q},$$

und wenn Q durch m teilbar ist:

(4) $$\alpha' \equiv r \pmod{m},$$

also nach (2) und (3)

$$r^2 \equiv 1 \pmod{m}$$

(5) $$(r-1)(r+1) \equiv 0 \pmod{m},$$

wir nehmen also Q durch m und m durch $\mathfrak{m}$ teilbar an; dann ist nach (5), wenn $\mathfrak{m}$, wie wir angenommen haben, ein Primideal oder eine Potenz eines solchen ist, entweder

(6) $$r \equiv 1 \quad \text{oder} \quad r \equiv -1 \pmod{\mathfrak{m}},$$

und aus (4) folgt:

(7) $$\alpha' \equiv \pm 1 \pmod{\mathfrak{m}};$$

folglich ist A' in A enthalten, und nach § 164, 11. ist also $\mathfrak{K}(A)$ in $\mathfrak{K}(A')$ enthalten. Da nun nach § 158 jeder Teilungskörper sich aus solchen zusammensetzen läßt, deren Teiler ein Primideal oder eine Potenz eines Primideals ist, so folgt:

6. Der Teilungskörper der elliptischen Funktionen ist zurückführbar auf Ordnungskörper und Kreisteilungskörper[1]).

---

[1]) Auf anderem Wege ist ein Teil dieses Satzes bewiesen in der Straßburger Dissertation von Daniel Bauer, „Über den Teilungskörper der elliptischen Funktionen mit singulärem Modul". Straßburg 1903.

FÜNFTES BUCH.

ALGEBRAISCHE FUNKTIONEN.

Vierundzwanzigster Abschnitt.

Algebraische Funktionen einer Variablen.

§ 170. Einleitendes.

Die Theorie der algebraischen Funktionen einer Veränderlichen ist der Ausgangspunkt der allgemeinen Untersuchungen von Abel über die neuen Transzendenten, die seitdem den Namen „Abelsche Funktionen" erhalten haben, und die höchste Verallgemeinerung der elliptischen Funktionen sind. Die Hauptprobleme dieser Theorie sind durch die Arbeiten von Riemann, Weierstrass, Clebsch, Brill und Noether zu einem gewissen Abschluß gebracht. Insbesondere hat Riemann in der Vorstellung der mehrblätterigen (Riemannschen) Flächen ein durch seine Anschaulichkeit außerordentlich wirksames Hilfsmittel für die Untersuchung dieser Funktionen geschaffen.

Alle diese Untersuchungen aber, die sich einerseits auf die Funktionentheorie, andererseits, wie bei Clebsch, Brill, Noether, auf die Methoden der rationalen Algebra (Theorie der Formen und Invarianten oder der algebraischen Kurven) stützen, müssen immer gewisse Einschränkungen machen, sie müssen gewisse „Ausnahmefälle" ausschließen und sich mit der Behandlung der sogenannten allgemeinen Fälle begnügen. Nicht unterworfen ist dieser Beschränkung die nach Analogie der Zahlentheorie von Dedekind und mir ausgearbeitete Theorie der algebraischen Funktionen, von der hier eine Übersicht gegeben werden soll[1].

[1]) Zur Literatur über algebraische und Abelsche Funktionen sei hier erwähnt: Abel, Mém. sur une propriété générale d'une classe très-étendue de fonctions transcendentes (1826 der Pariser Akademie vorgelegt, Werke, neue Ausgabe von Sylow und Lie, Bd. I, S. 145). Riemann, Theorie der Abelschen Funktionen, Crelles Journ., Bd. 54, 1857, Werke 2. Aufl., Nr. 88. Weierstrass, Vorlesungen 1875/76, Werke, Bd. IV. Clebsch, Über die

§ 171. Definition der algebraischen Funktionen.

Eine Variable θ heißt eine algebraische Funktion einer unabhängigen Veränderlichen z, wenn die beiden Variablen durch eine algebraische Gleichung

$$(1) \qquad F(\theta, z) = 0$$

miteinander verbunden sind. F bedeutet hierin einen Ausdruck von der Form

$$(2) \qquad F(\theta, z) = a_0\,\theta^n + a_1\,\theta^{n-1} + \cdots + a_{n-1}\,\theta + a_n,$$

dessen Koeffizienten $a_0, a_1, \ldots, a_n$ ganze rationale Funktionen von z ohne gemeinschaftlichen Teiler sind. Über die konstanten Koeffizienten in diesen Ausdrücken machen wir weiter keine Voraussetzung, als daß es reelle oder komplexe Zahlen sind [1]).

Wir setzen dabei die Funktion $F(\theta, z)$ in dem Sinne als irreduzibel voraus, daß sie nicht in Faktoren zerfallen soll, die selbst rationale Funktionen von θ und z sind.

Jede ganze Funktion $G(\theta, z)$ läßt sich nach Bd. I, § 20 nur auf eine Weise in irreduzible Faktoren zerlegen (abgesehen von konstanten Faktoren). Wir sagen, daß die Funktion $G(\theta, z)$

Anwendung der Abelschen Funktionen in der Geometrie, Crelles Journ., Bd. 63, 1864. Clebsch und Gordan, Theorie der Abelschen Funktionen, Leipzig 1866. Brill und Noether, Über die algebraischen Funktionen und ihre Anwendung in der Geometrie, Mathematische Annalen VII, 1874. Brill und Noether, Die Entwickelung der Theorie d[illegible] Funktionen, Bericht der Deutschen Mathematiker-Vereinigun[illegible] et Goursat, Théorie des fonctions algébriques, Paris 1895. [illegible]heoretischen Methoden: Kronecker, Über die Diskriminante algebraischer Funktionen, Crelles Journ., Bd. 91, 1881, und: Festschrift zu Kummers Doktor-Jubiläum, Crelles Journ., Bd. 92, 1881. Dedekind und Weber, Theorie der algebraischen Funktionen einer Veränderlichen, Crelles Journ., Bd. 92, 1879. Hensel und Landsberg, Theorie der algebraischen Funktionen einer Variablen, Leipzig 1902. Die Form der Theorie, die im folgenden dargestellt ist, stützt sich auf den in Bd. II, § 153 eingeführten Begriff der Funktionale, die in dieser Form bereits in einer von Wellstein angeregten Straßburger Dissertation von Rehfeld (1906) zur Behandlung eines speziellen Problems der Funktionentheorie angewandt wurden.

[1]) Es würde nirgends eine Lücke bleiben, wenn wir uns dabei auf algebraische Zahlen beschränken wollten. Betrachtet man θ, z als Cartesische Koordinaten in der Ebene, so stellt die Gleichung (1) eine algebraische Kurve dar, und man kann die Theorie dieser Kurven anwenden, wie es Clebsch und Gordan und Brill und Noether getan haben. Freilich haben dabei nur die reellen Werte dieser Variablen eine wirklich anschauliche Bedeutung.

dann und nur dann verschwinde, wenn unter ihren irreduziblen Faktoren die Funktion $F(\theta, z)$ vorkommt. Dies ist die Definition des Verschwindens, nach der, wenn man ganz korrekt sein wollte, eine jede Gleichung $G(\theta, z) = 0$ als Kongruenz nach dem Modul F aufzufassen wäre. Um nicht weitläufig zu sein, wollen wir aber diese Ausdrucksweise hier nicht brauchen.

Wenn wir die Gleichung (1) durch a_0 dividieren, so erhält sie die Form

(3) $$f(\theta, z) = \theta^n + b_1 \theta^{n-1} + b_2 \theta^{n-2} + \cdots + b_{n-1}\theta + b_n,$$

worin die $b_1, b_2, \ldots, b_n$ ganze oder gebrochene rationale Funktionen von z sind.

Das System aller ganzen und gebrochenen rationalen Funktionen $\Phi(\theta, z)$ von θ und z, in denen der Nenner nicht durch F teilbar ist, also nicht verschwindet, hat die Eigenschaft, sich durch Addition, Subtraktion, Multiplikation und Division (außer durch 0) zu reproduzieren, und bildet daher einen Körper algebraischer Funktionen (Bd. I, § 146), den ich mit Ω bezeichnen will.

Der Grad n der irreduziblen Gleichung (2) oder (3), also der Gleichung niedrigsten Grades, der θ genügt, heißt der Grad des algebraischen Körpers in bezug auf θ oder auch der Grad von θ.

Ist $\varphi(\theta)$ eine ganze Funktion von θ, deren Koeffizienten ganze oder gebrochene rationale Funktionen von z sind, so kann man durch Division eine Gleichung bilden:

$$\varphi(\theta) = f(\theta)\, q(\theta) + r(\theta),$$

worin $q(\theta)$ und $r(\theta)$ ebensolche Funktionen wie φ sind, von denen jedoch $r(\theta)$ höchstens vom Grade $n-1$ ist. Wegen (3) ist dann

(4) $$\varphi(\theta) = r(\theta).$$

Ist $\varphi(\theta)$ nicht durch $f(\theta)$ teilbar, so haben die beiden Funktionen keinen rationalen Teiler gemein, und man kann zwei Funktionen des Körpers $f_1(\theta)$, $\varphi_1(\theta)$ so bestimmen, daß

$$f(\theta) f_1(\theta) + \varphi(\theta)\, \varphi_1(\theta) = 1$$

wird (Bd. I, § 6). Da nun $f(\theta) = 0$ ist, so folgt hieraus:

(5) $$\varphi_1(\theta) = \frac{1}{\varphi(\theta)}.$$

Man kann also jede gebrochene Funktion von θ durch eine ganze Funktion von θ ersetzen und erhält so den Satz:

1. Jede Funktion ζ des Körpers Ω läßt sich auf eine einzige Weise in die Form setzen:

$$\zeta = x_0 + x_1\theta + x_2\theta^2 + \cdots + x_{n-1}\theta^{n-1}, \tag{6}$$

deren Koeffizienten $x_0, x_1, x_2, \ldots, x_{n-1}$ rationale Funktionen von z sind.

Daß dies überhaupt möglich ist, schließt man aus (4) und (5); daß es nur auf eine Weise möglich ist, folgt aus der Irreduzibilität von $f(\theta)$; denn hätte man zwei verschiedene Darstellungen einer und derselben Größe ζ in der Form (6), so würde ihre Differenz eine Gleichung für θ von niedrigerem als $n$tem Grade ergeben.

Wählt man n Funktionen des Körpers Ω beliebig aus:

$$\begin{aligned} \eta_1 &= x_0^{(1)} + x_1^{(1)}\theta + \cdots + x_{n-1}^{(1)}\theta^{n-1}, \\ \eta_2 &= x_0^{(2)} + x_2^{(2)}\theta + \cdots + x_{n-1}^{(2)}\theta^{n-1}, \\ & \cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_n &= x_0^{(n)} + x_1^{(n)}\theta + \cdots + x_{n-1}^{(n)}\theta^{n-1}, \end{aligned} \tag{7}$$

mit der einzigen Beschränkung, daß die Determinante

$$\Sigma \pm x_0^{(1)} x_1^{(2)} \ldots x_{n-1}^{(n)}$$

nicht identisch Null ist, so kann man durch Elimination der Potenzen von θ aus (6) und (7) jede Funktion ζ in Ω in die Form setzen:

$$\zeta = y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n, \tag{8}$$

deren Koeffizienten y_i rationale Funktionen von z sind.

Ein solches System von Funktionen $\eta_1, \eta_2, \ldots, \eta_n$ heißt eine Basis des Körpers Ω.

Damit ein Funktionensystem $\eta_1, \eta_2, \ldots, \eta_n$ eine Basis von Ω bilde, ist notwendig und hinreichend, daß keine Gleichung von der Form

$$y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n = 0$$

bestehe, in der die Koeffizienten $y_1, y_2, \ldots, y_n$ nicht sämtlich identisch verschwinden.

So bilden die Funktionen

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

eine Basis von Ω.

Der Übergang von einer Basis $\eta_1, \eta_2, \ldots, \eta_n$ zu einer anderen $\eta'_1, \eta'_2, \ldots, \eta'_n$ geschieht durch eine lineare Substitution:

(9) $$(\eta'_1, \eta'_2, \ldots, \eta'_n) = L(\eta_1, \eta_2, \ldots, \eta_n)$$

oder kürzer geschrieben

(10) $$(\eta'_i) = L(\eta_i),$$

worin L die Bedeutung hat

(11) $$L = \begin{pmatrix} l_{1,1}, & l_{1,2}, & \ldots, & l_{1,n} \\ l_{2,1}, & l_{2,2}, & \ldots, & l_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ l_{n,1}, & l_{n,2}, & \ldots, & l_{n,n} \end{pmatrix} \quad \text{(Bd. II, § 41).}$$

Die Elemente $l_{i,k}$ dieser Substitution sind rationale Funktionen von z.

Das System (η') ist dann und nur dann wieder eine Basis, wenn die Determinante $|L|$ dieser Substitution nicht verschwindet.

§ 172. Normen und Spuren.

Wählt man zur Darstellung der Funktionen in Ω eine beliebige Basis $\eta_1, \eta_2, \ldots, \eta_n$, so kann man, wenn ξ eine beliebige Funktion des Körpers ist, da die Produkte $\xi \eta_i$ im Körper enthalten sind, setzen:

(1) $$\begin{aligned} \xi \eta_1 &= y_{1,1} \eta_1 + y_{1,2} \eta_2 + \cdots + y_{1,n} \eta_n, \\ \xi \eta_2 &= y_{2,1} \eta_1 + y_{2,2} \eta_2 + \cdots + y_{2,n} \eta_n, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \xi \eta_n &= y_{n,1} \eta_1 + y_{n,2} \eta_2 + \cdots + y_{n,n} \eta_n, \end{aligned}$$

und daraus erhält man durch Elimination der η:

(2) $$\begin{vmatrix} y_{1,1} - \xi, & y_{1,2}, & \ldots, & y_{1,n} \\ y_{2,1}, & y_{2,2} - \xi, & \ldots, & y_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ y_{n,1}, & y_{n,2}, & \ldots, & y_{n,n} - \xi \end{vmatrix} = 0,$$

eine Gleichung, die nach Potenzen von ξ geordnet, die Gestalt erhält:

(3) $$\varphi(\xi) = \xi^n + b_1 \xi^{n-1} + \cdots + b_{n-1} \xi + b_n = 0,$$

in der $b_1, b_2, \ldots, b_n$ rationale Funktionen von z sind. Diese Koeffizienten sind von der Wahl der Basis η_i unabhängig. Denn die Gleichungen (1), durch die der Übergang von der Basis η_i

zu der Basis $\zeta \eta_i$ vermittelt wird, können wir nach der Bezeichnung (9), (10) des vorigen Paragraphen so darstellen:

(4) $$(\zeta \eta_i) = Y(\eta_i),$$

und demnach ergibt sich durch Übergang zu der Basis η'_i:

$$(\zeta \eta'_i) = L Y L^{-1} (\eta'_i).$$

Die Funktionen $b_1, b_2, \ldots, b_n$ sind also durch die Funktion ζ vollständig bestimmt.

Die Funktion

(5) $$(-1)^n b_n = \begin{vmatrix} y_{1,1}, & y_{1,2}, & \ldots, & y_{1,n} \\ y_{2,1}, & y_{2,2}, & \ldots, & y_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ y_{n,1}, & y_{n,2}, & \ldots, & y_{n,n} \end{vmatrix}$$

heißt die Norm der Funktion ζ und wird mit $N(\zeta)$ bezeichnet. Über sie gelten folgende Sätze:

1. Wenn ζ nicht identisch Null ist, so ist $N(\zeta)$ von Null verschieden.

Denn wenn die Determinante des Systems (1) verschwindet, so lassen sich rationale Funktionen $y_1, y_2, \ldots, y_n$, die nicht alle verschwinden, so bestimmen, daß

$$\zeta(y_1 \eta_1 + y_2 \eta_2 + \cdots + y_n \eta_n) = 0$$

wird, und dies fordert, da $\eta_1, \eta_2, \ldots, \eta_n$ eine Basis ist, $\zeta = 0$.

2. Ist ζ eine rationale Funktion von z, so ist ihre Norm die $n$te Potenz dieser Funktion.

Denn ist ζ rational, so reduzieren sich die Gleichungen (1) auf die Identitäten $\zeta \eta_i = \zeta \eta_i$. Es verschwinden also in der Determinante (5) alle Glieder mit Ausnahme der Diagonalglieder, und diese werden alle gleich ζ. Wir drücken diesen Satz durch die Formel aus:

$$N(a) = a^n.$$

3. Sind ζ, ζ' zwei Funktionen in Ω, so gilt der Satz

(6) $$N(\zeta \zeta') = N(\zeta) N(\zeta').$$

Denn ist nach (4):

$$(\zeta \eta_i) = Y(\eta_i), \quad (\zeta' \eta_i) = Y'(\eta_i),$$

so ist

$$(\zeta \zeta' \eta_i) = Y Y'(\eta_i),$$

und daraus folgt die Formel (6), weil die Determinante einer zusammengesetzten linearen Substitution, hier $Y Y'$, gleich dem Produkt der Determinante der Komponenten ist.

4. Aus 2. und 3. folgt, wenn ζ von Null verschieden ist:

$$N(\zeta)\,N\left(\frac{1}{\zeta}\right) = 1,$$

und daraus für irgend zwei ζ, ζ':

(7)
$$N\left(\frac{\zeta'}{\zeta}\right) = \frac{N(\zeta')}{N(\zeta)}.$$

5. Ist t eine unbestimmte oder variable Größe, und $\varphi(t)$ die Funktion, die nach (3) für $t = \zeta$ zu Null wird, so ist

(8)
$$\varphi(t) = N(t - \zeta).$$

Das ergibt sich aus (1) und (2). Denn ersetzt man in (1) ζ durch $\zeta - t$, so ist dies gleichbedeutend damit, daß man $y_{i,i}$ durch $y_{i,i} - t$ ersetzt und die übrigen $y_{i,k}$ ungeändert läßt.

Zerlegen wir die Funktion $\varphi(t)$, die eine rationale Funktion von t und z ist, in ein Produkt von irreduziblen Faktoren $\varphi_1(t)$, $\varphi_2(t)$, ... so muß einer dieser Faktoren für $t = \zeta$ verschwinden. Sei dies $\varphi_1(t)$, und

(9)
$$\varphi_1(t) = t^e + b'_1 t^{e-1} + \cdots + b'_{e-1} t + b'_e$$

sei vom Grade e. Es ist dann $\varphi_1(\zeta) = 0$ die Gleichung niedrigsten Grades, der ζ genügt, und aus ζ leitet man einen Körper Ω_1 ab, der in Ω enthalten ist und den Grad e hat. Jede Zahl η des Körpers Ω_1 kann, und zwar auf eine Art, in der Form dargestellt werden:

(10)
$$\eta = x_0 + x_1\zeta + \cdots + x_{e-1}\zeta^{e-1}.$$

Sei ferner

(11)
$$\theta^f + \eta_1\theta^{f-1} + \cdots + \eta_{f-1}\theta^{f-1} + \eta_f = 0$$

die Gleichung niedrigsten Grades mit Koeffizienten in Ω_1, der θ genügt, also f der Relativgrad von Ω in bezug auf Ω_1.

Durch die ef Funktionen

(12)
$$\zeta^h\theta^k \quad \begin{matrix} h = 0, 1, \ldots, e-1 \\ k = 0, 1, \ldots, f-1 \end{matrix}$$

kann jede Funktion des Körpers linear ausgedrückt werden, und zwischen ihnen besteht keine lineare Gleichung mit rational von z abhängigen Koeffizienten. Denn sonst würde θ oder ζ aus einer Gleichung von niedrigerem Grade als f oder e entstehen. Dem-

nach bilden die Funktionen (12) eine Basis des Körpers Ω, und es folgt

$$ef = n. \tag{13}$$

Es sind also e und f Teiler von n.

Bedeutet

$$\zeta_1, \zeta_2, \ldots, \zeta_e \tag{14}$$

eine Basis des Körpers Ω_1, so bilden die n Größen:

$$\zeta_1 \theta^k, \zeta_2 \theta^k, \ldots, \zeta_e \theta^k, \qquad k = 0, 1, 2, \ldots, f-1 \tag{15}$$

eine Basis von Ω. Bildet man die Substitution der e Größen:

$$(\zeta \zeta_i) = Y_1(\zeta_i), \tag{16}$$

so ist

$$(-1)^e b'_e = |Y_1| = N_1(\zeta) \tag{17}$$

die Norm von ζ im Körper Ω_1, und wenn man die Substitution für $(\zeta \zeta_i \theta_k)$ im Körper Ω mit der Basis (15) bildet, so ergibt sich

$$(\zeta \zeta_i \theta^k) = Y_1(\zeta_i)\, Y_1(\zeta_i \theta) \ldots Y_1(\zeta_i \theta^{e-1}),$$

woraus

$$N(\zeta) = |Y_1|^f. \tag{18}$$

Aus der Substitutionsdeterminante $|Y_1|$ leitet man die Funktion $\varphi_1(t)$ nach der Formel (2) ab, und es folgt also nach (18):

$$N(t - \zeta) = [\varphi_1(t)]^f, \tag{19}$$

und daraus:

6. Die Funktion $\varphi(t) = N(t - \zeta)$ ist entweder irreduzibel oder eine Potenz einer irreduziblen Funktion.

Ist der Exponent f dieser Potenz größer als 1, so ist der Körper Ω imprimitiv, Ω_1 ist ein Teilkörper, und Ω ist ein Körper vom Grade f über Ω_1 (Bd. I, § 151).

Ist $f = 1$, $e = n$, so heißt ζ eine primitive Funktion des Körpers Ω, und Ω_1 ist mit Ω identisch.

Wir kehren zu der Gleichung (2) oder (3) zurück, die, wie wir gesehen haben, von der Wahl der Basis unabhängig ist, und definieren den Koeffizienten

$$-b_1 = y_{1,1} + y_{2,2} + \cdots + y_{n,n} = S(\zeta) \tag{20}$$

als die Spur der Funktion ζ. Für die Spur ergeben sich aus der Definition die folgenden fundamentalen Sätze, in denen ζ, ζ' irgend zwei Funktionen in Ω, und x eine rationale Funktion bedeutet:

$$(21)\qquad \begin{aligned} S(0) &= 0, \\ S(1) &= n, \\ S(x\zeta) &= x\,S(\zeta), \\ S(\zeta + \zeta') &= S(\zeta) + S(\zeta'). \end{aligned}$$

Alle Spuren sind rationale Funktionen von z.

§ 173. Diskriminanten.

Ist $(\eta_1, \eta_2, \ldots, \eta_n) = (\eta_i)$ ein System von n Funktionen im Körper Ω, so sind die n^2 Spuren $S(\eta_i \eta_k)$ rationale Funktionen von z. Wir definieren als Diskriminante des Systems (η_i) die Determinante

$$(1)\qquad \Delta(\eta_1, \eta_2, \ldots, \eta_n) = \begin{vmatrix} S(\eta_1\eta_1), & S(\eta_1\eta_2), & \ldots, & S(\eta_1\eta_n) \\ S(\eta_2\eta_1), & S(\eta_2\eta_2), & \ldots, & S(\eta_2\eta_n) \\ \cdot & \cdot & \cdot & \cdot \\ S(\eta_n\eta_1), & S(\eta_n\eta_2), & \ldots, & S(\eta_n\eta_n) \end{vmatrix},$$

wofür wir auch kürzer $\Delta(\eta_i)$ schreiben.

Wir beweisen den Satz:

7. Die Diskriminante $\Delta(\eta_i)$ ist dann und nur dann von Null verschieden, wenn (η_i) eine Basis des Körpers Ω ist.

Nehmen wir, um ihn zu beweisen, zunächst an, daß $\Delta(\eta_i) = 0$ sei. Dann kann man nach einem elementaren Determinantensatz die rationalen Funktionen $y_1, y_2, \ldots, y_n$, ohne daß sie alle Null sind, so bestimmen, daß

$$(2)\qquad \begin{gathered} y_1 S(\eta_1\eta_k) + y_2 S(\eta_2\eta_k) + \cdots + y_n S(\eta_n\eta_k) = \\ S[\eta_k(y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n)] = 0 \\ (k = 1, 2, \ldots, n) \end{gathered}$$

ist. Bedeutet $x_1, x_2, \ldots, x_n$ ein beliebiges System rationaler Funktionen, und setzt man

$$(3)\qquad \begin{aligned} y_1\eta_1 + y_2\eta_2 + \cdots + y_n\eta_n &= \eta, \\ x_1\eta_1 + x_2\eta_2 + \cdots + x_n\eta_n &= \xi, \end{aligned}$$

so folgt aus (2) durch Multiplikation mit x_k und Summation:

$$(4)\qquad S(\xi\eta) = 0.$$

Ist nun (η_i) eine Basis, so kann ξ jede beliebige Funktion in Ω, also auch $1/\eta$ sein, und dann gibt die Formel (4) das widersprechende Resultat $S(1) = 0$; also kann die Diskriminante einer Basis (η_i) nicht verschwinden.

Um auch das Umgekehrte zu beweisen, nehmen wir an, es sei (η_i) eine Basis und

(5) $$(\eta_i') = X(\eta_i)$$

eine lineare Substitution. Das System (η_i') ist dann und nur dann gleichfalls eine Basis, wenn die Determinante $|X|$ dieser Substitution von Null verschieden ist (§ 171). Setzt man nach (5)

$$\eta_h' = x_{h,1}\eta_1 + x_{h,2}\eta_2 + \cdots + x_{h,n}\eta_n,$$

so wird

$$S(\eta_h'\eta_k') = \overset{i\,i'}{\Sigma} x_{h,i}x_{k,i'}\,S(\eta_i\eta_{i'}),$$

und indem man daraus die Determinante bildet:

(6) $$\varDelta(\eta_1', \eta_2', \ldots, \eta_n') = |X|^2 \varDelta(\eta_1, \eta_2, \ldots, \eta_n).$$

Ist also $\varDelta(\eta_i')$ von Null verschieden, so kann $|X|$ nicht verschwinden und (η_i') ist eine Basis. Damit ist 7. bewiesen.

Aus (6) ergibt sich noch nach der Definition der Norm in § 172, wenn man $\eta_i' = \zeta\eta_i$ setzt, und ζ eine beliebige Funktion in Ω ist:

(7) $$\varDelta(\zeta\eta_i) = N(\zeta)^2\varDelta(\eta_i).$$

§ 174. Die Potenzsummen.

Die Spuren der Potenzen von θ

(1) $$s_k = S(\theta^k)$$

sind nichts anderes als die Potenzsummen, die nach den Newtonschen Formeln berechnet werden können. Da wir aber hier nicht von den „Wurzeln" der Gleichung $f(\theta) = 0$ sprechen dürfen, die wir noch nicht haben, so müssen diese Formeln direkt aus der Definition der Spur abgeleitet werden.

Ist $f(\theta) = 0$ die den Körper Ω definierende Gleichung, so setzen wir

(2) $$f(t) = t^n + a_1 t^{n-1} + \cdots + a_{n-1}t + a_n$$

und bilden den Quotienten:

(3) $$\frac{f(t)}{t-\theta} = \eta_0 + \eta_1 t + \eta_2 t^2 + \cdots + \eta_{n-1}t^{n-1},$$

worin

(4) $$\begin{aligned} \eta_0 &= a_{n-1} + a_{n-2}\theta + \cdots + a_1\theta^{n-2} + \theta^{n-1}, \\ \eta_1 &= a_{n-2} + a_{n-3}\theta + \cdots + \theta^{n-2}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ \eta_{n-2} &= a_1 + \theta, \\ \eta_{n-1} &= 1. \end{aligned}$$

Zwischen diesen Funktionen bestehen die Relationen:

$$
(5) \qquad
\begin{aligned}
\theta\,\eta_0 &= \qquad\; - a_n\,\eta_{n-1},\\
\theta\,\eta_1 &= \eta_0 \;\; - a_{n-1}\,\eta_{n-1},\\
\theta\,\eta_2 &= \eta_1 \;\; - a_{n-2}\,\eta_{n-1},\\
&\cdots\cdots\cdots\\
\theta\,\eta_{n-1} &= \eta_{n-2} - a_1\,\eta_{n-1},
\end{aligned}
$$

und die $\eta_0, \eta_1, \ldots, \eta_{n-1}$ bilden eine Basis von Ω, da man durch (4) die Potenzen von θ linear durch die η_i ausdrücken kann.

Ist also ζ eine beliebige Funktion in Ω, so kann man setzen:

$$
(6) \qquad \zeta = y_0\,\eta_0 + y_1\,\eta_1 + \cdots + y_{n-1}\,\eta_{n-1}.
$$

Wir leiten aus $y_0, y_1, \ldots, y_{n-1}$ eine Fortsetzung der Reihe dieser rationalen Funktionen $y_n, y_{n+1}, y_{n+2}, \ldots$ ab, indem wir setzen:

$$
(7) \qquad a_n y_r + a_{n-1} y_{r+1} + \cdots + a_1 y_{r+n-1} + y_{r+n} = 0
$$
$$
(r = 0, 1, 2, \ldots).
$$

Dann ergibt sich aus (5) und (6):

$$
\begin{aligned}
\zeta\,\theta &= \eta_0 y_1 + \eta_1 y_2 + \cdots + \eta_{n-2} y_{n-1},\\
&\quad - \eta_{n-1}(a_n y_0 + a_{n-1} y_1 + \cdots + a_1\,y_{n-1}),\\
&= y_1\,\eta_0 + y_2\,\eta_1 + \cdots + y_n\,\eta_{n-1},
\end{aligned}
$$

und allgemein für ein positives r:

$$
(8) \qquad \zeta\,\theta^r = y_r\,\eta_0 + y_{r+1}\,\eta_1 + \cdots + y_{r+n-1}\,\eta_{n-1},
$$

wie man aus (5) und (7) durch den Schluß von r auf $r+1$ leicht bestätigt. Ordnet man diese Summe nach Potenzen von θ, so ergibt sich ein Ausdruck von der Form

$$
(9) \qquad \zeta\,\theta^r = x_{0,r} + x_{1,r}\,\theta + x_{2,r}\,\theta^2 + \cdots + x_{n-1,r}\,\theta^{n-1},
$$

worin

$$
(10) \qquad
\begin{aligned}
x_{0,r} &= y_r\,a_{n-1} + y_{r+1}\,a_{n-2} + \cdots + y_{r+n-2}\,a_1 + y_{r+n-1},\\
x_{1,r} &= y_r\,a_{n-2} + y_{r+1}\,a_{n-3} + \cdots + y_{r+n-1},\\
&\cdots\cdots\cdots\\
x_{n-2,r} &= y_r\,a_1 + y_{r+1},\\
x_{n-1,r} &= y_r.
\end{aligned}
$$

Nach der Definition der Spur [§ 172, (20)] ist aber

$$
(11) \qquad
\begin{aligned}
S(\zeta) &= x_{0,0} + x_{1,1} + \cdots + x_{n-1,\,n-1},\\
&= y_0\,a_{n-1} + 2\,y_1\,a_{n-2} + 3\,y_2\,a_{n-3} + \cdots + n\,y_{n-1}.
\end{aligned}
$$

Will man diesen Ausdruck auf $\zeta = \eta_r$ anwenden, so hat man $y_r = 1$, die übrigen $y = 0$ zu setzen und erhält

$$
S(\eta_r) = (r + 1)\,a_{n-r-1}, \quad S(\eta_{n-1-r}) = (n - r)\,a_r,
$$

und folglich, solange $r \gtreqless n$ ist, nach (4) mit der Bezeichnung (1):

(12) $(n - r)\, a_r = a_r\, s_0 + a_{r-1}\, s_1 + \cdots + a_1\, s_{r-1} + s_r,$

und wenn man die Spur von $\theta^r f(\theta) = 0$ nimmt:

(13) $0 = a_n\, s_r + a_{n-1}\, s_{r+1} + \cdots + a_1\, s_{r+n-1} + s_{r+n}.$

Dies sind die Newtonschen Formeln (Bd. I, § 46).

Bezeichnen wir mit

$$f'(t) = n\, t^{n-1} + (n-1)\, a_1\, t^{n-2} + \cdots + 2\, a_{n-2}\, t + a_{n-1}$$

die abgeleitete Funktion von $f(t)$, multiplizieren die Gleichung (12) mit θ^{n-r-1} und summieren von $r = 0$ bis $r = n - 1$, so folgt:

(14) $f'(\theta) = \eta_0\, s_0 + \eta_1\, s_1 + \cdots + \eta_{n-1}\, s_{n-1},$

und wenn man für irgend ein positives k die Gleichungen (12) mit $\theta^{n-r+k-1}$ multipliziert und noch so viele von den Gleichungen (13) hinzunimmt, bis $n - r + k - 1$ anfängt, negativ zu werden, so ergibt sich:

(15) $\theta^k f'(\theta) = \eta_0\, s_k + \eta_1\, s_{k+1} + \cdots + \eta_{n-1}\, s_{k+n-1}.$

Um die Norm von $f'(\theta)$ zu bilden, hätte man in diesen Gleichungen zunächst die Basis $\eta_0, \eta_1, \ldots, \eta_{n-1}$ durch die Substitution (2) durch $(1, \theta, \theta^2, \ldots, \theta^{n-1})$ auszudrücken, dann die Gleichung (15) für $k = 0, 1, \ldots, n-1$ zu bilden und die Determinante dieses Systems zu nehmen. Statt dessen kann man die Determinante in bezug auf die η nehmen, und dann mit der Substitutionsdeterminante:

$$\begin{vmatrix} a_{n-1}, & a_{n-2}, & \ldots, & a_1, & 1 \\ a_{n-2}, & a_{n-3}, & \ldots, & 1, & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ 1, & 0, & \ldots, & 0, & 0 \end{vmatrix} = (-1)^{\frac{1}{2} n(n+1)}$$

multiplizieren. Dadurch erhält man

(16) $$N[f'(\theta)] = (-1)^{\frac{1}{2} n(n+1)} \begin{vmatrix} s_0, & s_1, & \ldots, & s_{n-1} \\ s_1, & s_2, & \ldots, & s_n \\ \cdot & \cdot & \cdot & \cdot \\ s_{n-1}, & s_n, & \ldots, & s_{2n-2} \end{vmatrix}.$$

Diese Determinante ist aber nach der Definition der Diskriminante (§ 173):

$$\varDelta(1, \theta, \theta^2, \ldots, \theta^{n-1}),$$

und wir haben also:

(17) $$N f'(\theta) = (-1)^{\frac{1}{2} n(n+1)}\, \varDelta(1, \theta, \theta^2, \ldots, \theta^{n-1}).$$

In der Betrachtung dieses Abschnittes haben wir, dem Hauptziel der Untersuchung entsprechend, die Koeffizienten $a_1, a_2, \ldots, a_n$ als rationale Funktionen von z betrachtet. Alles bleibt aber vollständig ungeändert, wenn wir für diese Größen irgend einen Rationalitätsbereich festsetzen.

§ 175. Ganze Funktionen von z.

Jede Funktion ω des Körpers Ω genügt, wie wir gesehen haben, einer Gleichung niedrigsten Grades:

$$(1) \qquad \omega^e + b_1\omega^{e-1} + b_2\omega^{e-2} + \cdots + b_e = 0,$$

deren Koeffizienten $b_1, b_2, \ldots, b_e$ rationale Funktionen von z sind.

1. Wenn diese Koeffizienten ganze rationale Funktionen von z sind, so heißt ω eine ganze algebraische oder kurz eine ganze Funktion von z.

Über die ganzen algebraischen Funktionen gelten die nämlichen Sätze, wie über die ganzen Zahlen (Bd. II, § 149).

Setzen wir

$$(2) \qquad \varphi(t) = t^e + b_1 t^{e-1} + b_2 t^{e-2} + \cdots + b_e,$$

so ist, wie wir in § 172 gesehen haben,

$$(3) \qquad N(t-\omega) = \varphi(t)^f \quad (ef = n)$$

eine ganze Potenz von $\varphi(t)$. Wenn wir daher $N(t-\omega)$ nach Potenzen von t ordnen, so werden die Koeffizienten alle wieder ganze rationale Funktionen, also insbesondere:

2. Die Norm und die Spur einer ganzen Funktion ω sind ganze rationale Funktionen von z.

3. Eine rationale Funktion von z ist nur dann eine ganze algebraische Funktion, wenn sie eine ganze rationale Funktion ist.

Denn ist $\omega = -b$ rational, so ist $e = 1$ und $\omega + b = 0$ die Gleichung niedrigsten Grades für ω, also ω nur dann ganz, wenn b ganz und rational ist.

4. Jede Funktion η in Ω kann durch Multiplikation mit einer von Null verschiedenen rationalen Funktion von z in eine ganze algebraische Funktion verwandelt werden.

Denn jede Funktion η genügt einer Gleichung niedrigsten Grades:

$$(4) \qquad b_0\eta^e + b_1\eta^{e-1} + \cdots + b_{e-1}\eta + b_e = 0,$$

und wenn man mit b_0^{e-1} multipliziert und $b_0 \eta = \omega$ setzt, so erhält man eine Gleichung von der Form (1).

5. Eine Funktion ω des Körpers Ω ist eine ganze Funktion, wenn sie irgend einer Gleichung

$$\psi(\omega) = \omega^m + c_1 \omega^{m-1} + \cdots + c_{m-1}\omega + c_m = 0 \tag{5}$$

genügt, in der $c_1, c_2, \ldots, c_m$ ganze rationale Funktionen sind, wenn dies auch nicht die Gleichung niedrigsten Grades ist.

Denn ist $\varphi(\omega) = 0$ die Gleichung niedrigsten Grades für ω, so muß $\psi(t)$ für ein variables t durch $\varphi(t)$ teilbar sein. Das ist einfach der Inhalt der Gleichung (5). Es ist also

$$\psi(t) = \chi(t)\,\varphi(t),$$

worin $\psi(t)$ ebenfalls eine ganze Funktion von t ist. Wenn nun, wie vorausgesetzt, $\psi(t)$ ganze Koeffizienten hat, so müssen nach einem Satz von Gauss auch die Koeffizienten von $\varphi(t)$ und von $\chi(t)$ ganze Funktionen sein. Vgl. Bd. I, § 2, § 20, § 148[1]).

Hieraus ergibt sich der folgende Hauptsatz:

6. Summe, Differenz, Produkt zweier ganzer Funktionen in Ω sind wieder ganze Funktionen.

Sind nämlich ω', ω'' zwei ganze Funktionen in Ω, die den Gleichungen genügen:

$$\begin{aligned} &\omega'^{n'} + b_1' \omega'^{n'-1} + \cdots + b_{n'-1}'\omega' + b_{n'}' = 0, \\ &\omega''^{n''} + b_1'' \omega''^{n''-1} + \cdots + b_{n''-1}''\omega'' + b_{n''}'' = 0, \end{aligned} \tag{6}$$

so bezeichne man mit

$$\omega_1, \omega_2, \ldots, \omega_m$$

die Produkte

$$\omega'^{\nu'} \omega''^{\nu''}; \quad \begin{aligned} \nu' &= 0, 1, \ldots, n' - 1, \\ \nu'' &= 0, 1, \ldots, n'' - 1, \end{aligned}$$

und mit ω eine der drei Funktionen $\omega' \pm \omega''$, $\omega'\omega''$, dann kann man mit Hilfe der Gleichungen (6) setzen:

$$\begin{aligned} \omega\omega_1 &= x_{1,1}\omega_1 + \cdots + x_{1,m}\omega_m, \\ &\cdots\cdots\cdots\cdots \\ \omega\omega_m &= x_{m,1}\omega_1 + \cdots + x_{m,m}\omega_m, \end{aligned} \tag{7}$$

[1]) Bei diesem Beweis braucht nicht die Zerlegbarkeit der ganzen rationalen Funktionen in lineare Faktoren vorausgesetzt zu werden, sondern nur die Zerlegbarkeit in irreduzible Faktoren. Man kann also für die Zahlenkoeffizienten noch einen beliebigen Rationalitätsbereich festsetzen. Wir werden aber in der Folge die Zerlegbarkeit einer ganzen rationalen Funktion von z in lineare Faktoren, d. h. den Fundamentalsatz der Algebra, doch voraussetzen müssen.

wo $m = n' n''$ ist, und die $x_{\nu, \nu'}$ ganze rationale Funktionen von z sind. Aus (7) ergibt sich durch Elimination der ω_i:

$$\begin{vmatrix} x_{1,1} - \omega, & x_{1,2}, & \ldots, & x_{1,m} \\ x_{2,1}, & x_{2,2} - \omega, & \ldots, & x_{2,m} \\ \cdot & \cdot & \cdot & \cdot \\ x_{m,1}, & x_{m,2}, & \ldots, & x_{m,m} - \omega \end{vmatrix} = 0,$$

und dies ist eine Gleichung für ω von der Form (5).

Durch wiederholte Anwendung dieses Satzes folgt, daß jede ganze rationale Funktion von ganzen Funktionen wieder eine ganze Funktion ist.

7. Eine ganze Funktion ω heißt durch eine ganze Funktion ω' teilbar, wenn eine dritte ganze Funktion ω'' existiert, so daß

(8) $$\omega = \omega' \omega''$$

ist.

Aus dieser Definition ergibt sich ohne weiteres:

Ist ω teilbar durch ω' und ω' teilbar durch ω'', so ist auch ω durch ω'' teilbar.

Sind ω' und ω'' durch ω teilbar, so ist auch $\omega' \pm \omega''$ durch ω teilbar.

Sind $\omega_1, \omega_2, \omega_3, \ldots$ durch ω teilbar und $\omega_1', \omega_2', \omega_3', \ldots$ beliebige ganze Funktionen, so ist auch

$$\omega_1 \omega_1' + \omega_2 \omega_2' + \omega_3 \omega_3' + \cdots$$

durch ω teilbar.

§ 176. Minimalbasis und Körperdiskriminante.

Da man jede Funktion des Körpers Ω durch Multiplikation mit einer ganzen rationalen Funktion in eine ganze algebraische Funktion von z verwandeln kann, so gibt es auch Körperbasen, die aus ganzen Funktionen bestehen (z. B. nach der Bezeichnung in § 171, (2) die Potenzen von $a_0 \theta$).

Ist nun

(1) $$\omega_1, \omega_2, \ldots, \omega_n$$

eine solche aus ganzen Funktionen bestehende Basis, so ist jede in der Form

(2) $$\omega = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n$$

enthaltene Funktion, wenn die $x_1, x_2, \ldots, x_n$ ganze rationale Funktionen sind, eine ganze Funktion in Ω. Es ist aber nicht gesagt, daß auch umgekehrt in der Form (2) mit ganzen Koeffizienten x_i alle ganzen Funktionen in Ω enthalten sind.

Gibt es also ganze Funktionen in der Form (2), in der die x_i nicht alle ganze rationale Funktionen sind, so können wir eine ganze Funktion finden:

$$\frac{x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n}{z - c},$$

in der die x_i ganz und nicht alle durch $z - c$ teilbar sind. Reduzieren wir die x_i auf ihre konstanten Reste (nach $z - c$), so ergibt sich eine ganze Funktion ω in der Form:

$$(3) \qquad \omega = \frac{c_1 \omega_1 + c_2 \omega_2 + \cdots + c_n \omega_n}{z - c},$$

in der die Konstanten $c_1, c_2, \ldots, c_n$ jedenfalls nicht alle verschwinden. Ist etwa c_1 von Null verschieden, so können wir ω_1 durch $\omega, \omega_2, \ldots, \omega_n$ ausdrücken und erhalten eine neue ganzzahlige Basis von Ω:

$$(4) \qquad \omega, \omega_2, \ldots, \omega_n.$$

Für die Diskriminante ergibt sich aber nach § 173, (6) die Beziehung:

$$(5) \qquad \Delta(\omega, \omega_2, \ldots, \omega_n) = \frac{c_1^2}{(z - c)^2} \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Beide Diskriminanten sind ganze rationale Funktionen von z, aber die Diskriminante der Basis (4) ist von niedrigerem Grade als die Diskriminante der Basis (1).

Wenn wir auf diese Weise fortfahren, den Grad der Diskriminante zu erniedrigen, müssen wir schließlich zu einer aus ganzen Funktionen bestehenden Basis $\omega_1, \omega_2, \ldots, \omega_n$ kommen von der Eigenschaft, daß in der Form (2) mit ganzen rationalen x_i alle und nur die ganzen Funktionen in Ω ausgedrückt sind.

8. Definition: Eine ganzzahlige Basis $\omega_1, \omega_2, \ldots, \omega_n$ des Körpers Ω heißt eine Minimalbasis, wenn in der Form

$$(6) \qquad \omega = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n$$

mit ganzen rationalen $x_1, x_2, \ldots, x_n$ alle ganzen Funktionen des Körpers Ω darstellbar sind.

Eine solche Minimalbasis existiert also immer.

9. Ein aus einer Minimalbasis $\omega_1, \omega_2, \ldots, \omega_n$ abgeleitetes System ganzer Funktionen

$$\omega'_\nu = x_{\nu,1}\omega_1 + x_{\nu,2}\omega_2 + \cdots + x_{\nu,n}\omega_n, \tag{7}$$
$$\nu = 1, 2, \ldots, n$$

ist dann und nur dann eine Minimalbasis, wenn die Determinante

$$X = \Sigma \pm x_{1,1}\, x_{2,2} \ldots x_{n,n} \tag{8}$$

eine von Null verschiedene Konstante ist.

Denn hat diese Determinante, die eine rationale Funktion von z ist, einen Linearfaktor $z - c$, so kann man die Konstanten $c_1, c_2, \ldots, c_n$ so bestimmen, daß die n ganzen rationalen Funktionen

$$c_1 x_{1,\nu} + c_2 x_{2,\nu} + \cdots + c_n x_{n,\nu}$$

durch $z - c$ teilbar werden, ohne daß alle c_i verschwinden. Dann ist aber

$$\frac{c_1\omega'_1 + c_2\omega'_2 + \cdots + c_n\omega'_n}{z - c}$$

eine ganze Funktion, und $\omega'_1, \omega'_2, \ldots, \omega'_n$ keine Minimalbasis.

Für die Diskriminante erhält man aus (7) nach § 173, (6)

$$\varDelta(\omega'_1, \omega'_2, \ldots, \omega'_n) = X^2 \varDelta(\omega_1, \omega_2, \ldots, \omega_n). \tag{9}$$

Daraus folgt:

10. Die Diskriminante einer Minimalbasis ist, von einem konstanten Faktor abgesehen, von der besonderen Wahl der Basis unabhängig.

Die Diskriminante einer Minimalbasis hat unter allen Diskriminanten aus ganzen Funktionen gebildeter Basen den niedrigsten Grad (daher der Name Minimalbasis). Es ist eine durch den Körper selbst, abgesehen von einem konstanten Faktor, eindeutig bestimmte ganze rationale Funktion von z. Sie wird daher auch die Diskriminante des Körpers Ω genannt und mit $\varDelta(\Omega)$ bezeichnet.

Fünfundzwanzigster Abschnitt.

Funktionale.

§ 177. Rationale Funktionale.

Wir übertragen nun den Begriff des Funktionals, der uns im 17. Abschnitt des zweiten Bandes zur Begründung der Theorie der algebraischen Zahlen gedient hat, auf die algebraischen Funktionen.

Wir adjungieren also dem Körper Ω beliebige Variable und rechnen damit nach den Regeln der Buchstabenrechnung. Es entsteht so ein erweiterter Körper $\overline{\Omega}$, dessen Elemente Funktionale heißen. Der Körper $\overline{\Omega}$ selbst heißt der Funktionalkörper. Die Variablen sind hier nicht im Sinne der Analysis als Zeichen für veränderliche Zahlen, sondern als bloße Rechnungssymbole aufzufassen, und sind wohl zu unterscheiden von den Variablen z, θ des Körpers Ω. Wir wollen diese Hilfsvariablen die Funktionalvariablen nennen.

Aus dem Körper Z der rationalen Funktionen von z entsteht durch Adjunktion der Variablen der Körper $\overline{Z}$ der rationalen Funktionale.

Eine ganze rationale Funktion der Variablen:

$$\Phi(u, v, w, \ldots)$$

mit ganzen rationalen Funktionen von z als Koeffizienten heißt eine ganze Funktion in Z. Der größte gemeinschaftliche Teiler der Koeffizienten von Φ heißt der Teiler der Funktion, und die Funktion heißt primitiv, wenn die Koeffizienten keinen gemeinschaftlichen Teiler haben. Die primitiven rationalen Funktionen und ihre Quotienten werden auch Einheiten im Körper $\overline{Z}$ genannt.

Die Quotienten ganzer Funktionen in Z sind die Funktionale in $\overline{Z}$. Jedes Funktional $\overline{A}$ in $\overline{Z}$ kann in die Form gesetzt werden:

$$(1) \qquad \overline{A} = \frac{\Phi_1}{\Phi_2} = a\frac{E_1}{E_2} = aE,$$

worin Φ_1, Φ_2, E_1, E_2 ganze Funktionen in Z sind, darunter die Einheiten E_1, E_2, und E ist eine Einheit in $\overline{Z}$, die sich als gebrochene Funktion darstellt. a ist der Quotient der Teiler von Φ_1 und Φ_2, also eine ganze oder gebrochene rationale Funktion von z.

Die Funktionen a und E in der Formel (1) sind durch $\overline{A}$ völlig bestimmt, abgesehen von konstanten Faktoren, die hier die Rolle der numerischen Einheiten spielen. Wir wollen a die „Absolute" von $\overline{A}$ nennen. Es gilt dann der Satz:

1. Die Absolute eines Produktes ist gleich dem Produkt der Absoluten der Faktoren,

und wir definieren:

2. Ein rationales Funktional heißt ganz, wenn seine Absolute eine ganze Funktion von z ist.

Aus 1. folgt, daß das Produkt zweier ganzer Funktionale in $\overline{Z}$ wieder ein ganzes Funktional ist. Dasselbe folgt auch für die Summe und Differenz zweier ganzer Funktionale $\overline{A}_1$, $\overline{A}_2$ in $\overline{Z}$. Setzen wir nämlich:

$$\overline{A}_1 = a_1\frac{E_1}{E}, \quad \overline{A}_2 = \frac{a_2 E_2}{E},$$

$$\overline{A}_1 \pm \overline{A}_2 = \frac{a_1 E_1 \pm a_2 E_2}{E},$$

worin a_1, a_2 ganze rationale Funktionen von z sind; E_1, E_2, E ganze Einheiten, so ist die Absolute von $\overline{A}_1 \pm \overline{A}_2$ der Teiler der ganzen Funktion $a_1 E_1 \pm a_2 E_2$, also auch eine ganze Funktion von z. Also gilt der Satz:

3. Summe, Differenz und Produkt zweier ganzer Funktionale in $\overline{Z}$ sind wieder ganze rationale Funktionale.

Alle Einheiten und deren Reziproken sind nach der Definition als ganz zu bezeichnen. Ist die Absolute eines ganzen rationalen Funktionals $\overline{A}$ linear ($= z - c$), so heißt $\overline{A}$ ein rationales Primfunktional oder ein Primfunktional in $\overline{Z}$.

4. Jedes ganze rationale Funktional läßt sich in Primfaktoren zerlegen und zwar, von Einheitsfaktoren abgesehen, nur auf eine Weise.

Ist ein Produkt von ganzen Funktionalen in $\overline{Z}$ durch ein Primfunktional teilbar, so ist wenigstens einer der Faktoren durch dieses Primfunktional teilbar.

§ 178. Funktionale des Körpers $\overline{\Omega}$.

Ein Funktional des Körpers $\overline{\Omega}$ ist ein Ausdruck von der Form:

(1) $$\overline{\omega} = \overline{x}_0 + \overline{x}_1 \theta + \cdots + \overline{x}_{n-1} \theta^{n-1},$$

wo θ die den Körper Ω erzeugende algebraische Funktion ist, und $\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{n-1}$ rationale Funktionale sind. $\overline{\omega}$ ist nur dann $= 0$, wenn alle Koeffizienten $\overline{x}_0, \overline{x}_1, \ldots, \overline{x}_{n-1}$ verschwinden.

Jedes Funktional, das in bezug auf θ von höherem als dem $(n-1)$ten Grad ist, kann durch den Rest der Division durch $f(\theta)$ ersetzt, also auf den $(n-1)$ten Grad reduziert werden, und der Quotient zweier Ausdrücke (1), in der der Nenner nicht $= 0$ ist, kann wie in § 171, 1. auf die Form (1) gebracht werden.

Nimmt man eine beliebige Basis

$$\omega_1, \omega_2, \ldots, \omega_n$$

des Körpers Ω, so kann $\overline{\omega}$ auch in die Form

(2) $$\overline{\omega} = \overline{x}_1 \omega_1 + \overline{x}_2 \omega_2 + \cdots + \overline{x}_n \omega_n$$

gesetzt werden. Wendet man dies auf die Produkte $\overline{\omega}\omega_i$ an und setzt

(3) $$\overline{\omega}\omega_i = \overline{x}_{i,1} \omega_1 + \overline{x}_{i,2} \omega_2 + \cdots + \overline{x}_{i,n} \omega_n,$$

worin die $\overline{x}_{i,n}$ rationale Funktionale sind, so ergibt sich für $\overline{\omega}$ eine Gleichung:

(4) $$\begin{vmatrix} \overline{x}_{1,1} - \overline{\omega}, & \overline{x}_{1,2}, & \ldots, & \overline{x}_{1,n} \\ \overline{x}_{2,1}, & \overline{x}_{2,2} - \overline{\omega}, & \ldots, & \overline{x}_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ \overline{x}_{n,1}, & \overline{x}_{n,2}, & \ldots, & \overline{x}_{n,n} - \overline{\omega} \end{vmatrix} = 0,$$

also:

5. Jedes Funktional in $\overline{\Omega}$ genügt einer Gleichung

(5) $$\varphi(\overline{\omega}) = 0,$$

worin

(6) $$\varphi(t) = t^n + \overline{A}_1 t^{n-1} + \overline{A}_2 t^{n-2}, \cdots + \overline{A}_n$$

eine rationale Funktion $n$ten Grades von t ist, deren Koeffizienten $\overline{A}_1, \overline{A}_2, \ldots, \overline{A}_n$ Funktionale des Körpers $\overline{Z}$ sind.

Wir definieren die Norm und die Spur des Funktionals wie in § 172:

$$(7) \qquad N(\overline{\omega}) = \begin{vmatrix} \overline{x}_{1,1}, & \overline{x}_{1,2}, & \ldots, & \overline{x}_{1,n} \\ \overline{x}_{2,1}, & x_{2,2}, & \ldots, & \overline{x}_{2,n} \\ \cdot & \cdot & \cdot & \cdot \\ \overline{x}_{n,1}, & \overline{x}_{n,2}, & \ldots, & \overline{x}_{n,n} \end{vmatrix}$$

$$(8) \qquad S(\overline{\omega}) = \overline{x}_{1,1} + \overline{x}_{2,2} + \cdots + \overline{x}_{n,n},$$

und die Sätze § 172, (6) und (21) gelten unverändert auch von den Normen und Spuren der Funktionale.

Es ist dann, wie in § 172, (8),

$$(9) \qquad \varphi(t) = N(t - \overline{\omega}),$$

und die Diskriminante eines Funktionalsystems ist wie in § 173, (1) erklärt, und wenn das Funktional $\overline{\omega}$ in einem in $\overline{\Omega}$ enthaltenen Körper $e$ten Grades $\overline{\Omega}_1$ enthalten ist, so genügt $\overline{\omega}$ einer Gleichung $e$ten Grades $\varphi_1(t) = 0$. Wie in § 172, (19) wird bewiesen, daß

$$\varphi(t) = [\varphi_1(t)]^f \quad (n = ef)$$

eine Potenz von $\varphi_1(t)$ ist.

§ 179. Ganze Funktionale des Körpers $\overline{\Omega}$.

6. Definition. Ein Funktional $\overline{\omega}$ in $\overline{\Omega}$ heißt ganz, wenn es einer Gleichung:

$$(1) \qquad F(\overline{\omega}) = \overline{\omega}^m + \overline{A}_1 \overline{\omega}^{m-1} + \cdots + \overline{A}_{m-1}\overline{\omega} + \overline{A}_m = 0$$

genügt, deren Koeffizienten $\overline{A}_1, \ldots, \overline{A}_m$ ganze rationale Funktionale sind.

Aus dem Gaussschen Satz (Bd. I, § 2) folgt, da man nach § 177 die Primfaktoren in $\overline{Z}$ kennt, daß, wenn $F(t)$ in $\overline{Z}$ reduzibel ist, auch jede in $F(t)$ aufgehende Funktion ganze Koeffizienten hat, insbesondere also auch die Gleichung niedrigsten Grades $\varphi(\overline{\omega}) = 0$, der $\overline{\omega}$ genügt.

Die notwendige und hinreichende Bedingung für ein ganzes Funktional $\overline{\omega}$ ist also die, daß

$$N(t - \overline{\omega})$$

bei Ordnung nach Potenzen von t ganze rationale Funktionale zu Koeffizienten hat.

Wie in § 175 beweist man die Sätze:

7. Summe, Differenz, Produkt von ganzen Funktionalen in $\bar{\Omega}$ sind wieder ganze Funktionale.

8. Ist $\bar{\omega}$ ein ganzes Funktional in $\bar{\Omega}$ nach der Definition 6. und zugleich rational, so ist es ein ganzes Funktional in $\bar{Z}$ (nach der Definition 2.).

9. Ist $\bar{\omega}$ ein ganzes Funktional in $\bar{\Omega}$, so ist $N(\bar{\omega})$ ein ganzes Funktional in $\bar{Z}$, und die Absolute von $N(\bar{\omega})$ heißt die „absolute Norm von $\bar{\omega}$".

Die absolute Norm von $\bar{\omega}$ ist also eine Funktion in Z.

Bezeichnen wir die absolute Norm mit $N_a(\bar{\omega})$, so gilt der Satz:

$$N_a(\bar{\omega}\,\bar{\omega}') = N_a(\bar{\omega})\,N_a(\bar{\omega}'). \tag{2}$$

§ 180. Teilbarkeit von Funktionalen. Einheiten.

Es sind nun die Sätze von Bd. II, § 155 mit ganz geringen Modifikationen, auf die im folgenden aufmerksam gemacht ist, zu wiederholen. Zur Vereinfachung des Ausdruckes sollen hier mit den kleinen griechischen Buchstaben ganze Funktionale in $\bar{\Omega}$, mit den kleinen lateinischen Buchstaben ganze Funktionale in $\bar{Z}$ bezeichnet sein. Dann haben wir:

1. Definition: Wenn β von Null verschieden ist, so heißt α durch β teilbar, wenn $\alpha/\beta = \gamma$ ein ganzes Funktional in $\bar{\Omega}$ ist.

2. Sind $\xi, \eta, \ldots$ beliebige ganze Funktionale in $\bar{\Omega}$ und $\alpha, \beta, \ldots$ durch δ teilbar, so ist auch

$$\xi\alpha + \eta\beta + \cdots$$

durch δ teilbar.

3. Definition: Ein ganzes Funktional ε, dessen Reziprokes $1/\varepsilon$ ganz ist, d. h. ein Teiler der Zahl 1 heißt eine Einheit in $\bar{\Omega}$. Eine Einheit ist Teiler eines jeden ganzen Funktionals. Produkt und Quotient zweier Einheiten sind wieder Einheiten.

4. Zwei ganze Funktionale α, β, die gegenseitig durcheinander teilbar sind, heißen assoziiert. Ihr Quotient $\alpha/\beta = \varepsilon$ ist eine Einheit. Zwei Funktionale α und $\alpha\varepsilon$ sind assoziiert.

5. Ist α teilbar durch β, so ist jedes mit α assoziierte Funktional teilbar durch jedes mit β assoziierte Funktional.

6. Sind zwei ganze Funktionale mit einem dritten assoziiert, so sind sie auch untereinander assoziiert.

7. Die Norm $N(\alpha)$ ist durch α teilbar.

Dies folgt aus der Gleichung (6), § 178: $\varphi(\alpha) = 0$, deren letzter Koeffizient $\bar{A}_n = \pm N(\alpha)$ ist. Denn danach ist:

$$\pm N(\alpha) = \alpha(\alpha^{n-1} + \bar{A}_1 \alpha^{n-2} + \cdots + \bar{A}_{n-1}).$$

8. Ein ganzes Funktional, dessen absolute Norm eine Konstante ist, ist eine Einheit, und umgekehrt ist die absolute Norm einer Einheit ε eine von Null verschiedene Konstante.

Denn wenn ε eine Einheit ist, so sind

$$N(\varepsilon) \text{ und } N\left(\frac{1}{\varepsilon}\right) = \frac{1}{N(\varepsilon)}$$

ganze Funktionale in $\bar{Z}$; folglich $N(\varepsilon)$ eine Einheit in $\bar{Z}$. Umgekehrt ist $N(\varepsilon)$ durch ε teilbar, also, wenn $N(\varepsilon)$ eine Einheit in $\bar{Z}$ ist, ε ein Teiler von 1, d. h. eine Einheit.

9. Es gibt ganze rationale Funktionen von z, z. B. die absolute Norm von α, die durch α teilbar sind. Ist a eine durch α teilbare ganze rationale Funktion von z von möglichst niedrigem Grade, so ist jede andere durch α teilbare ganze rationale Funktion von z durch a teilbar.

§ 181. Größter gemeinschaftlicher Teiler.

Sind $\alpha, \beta, \ldots$ ganze Funktionale in $\bar{\Omega}$ und $x, y, \ldots$ Variable, die in $\alpha, \beta, \ldots$ nicht vorkommen, so ist

(1) $$\delta = \alpha x + \beta y + \cdots$$

nach § 180, 2. ebenfalls ein ganzes Funktional, und zwar ist δ teilbar durch jeden gemeinsamen Teiler von $\alpha, \beta, \ldots$ Sind $x_0, y_0, \ldots$ beliebige ganze Funktionen oder Funktionale in $\bar{Z}$, so ist, wie jetzt bewiesen werden soll,

(2) $$\delta_0 = \alpha x_0 + \beta y_0 + \cdots$$

durch δ teilbar. Denn bezeichnen wir die absolute Norm von δ mit D, so ist

(3) $$N(\delta) = D E(x, y, \ldots) = D E,$$

und $E(x, y, \ldots)$ ist eine Einheit in $\bar{Z}$, zugleich aber eine ganze homogene Funktion der Variablen $x, y, \cdots$

Bedeutet t eine neue Variable, so ist

$$N(\delta t - \delta_0) = D E(x t - x_0, y t - y_0, \ldots),$$

also, wenn man nach absteigenden Potenzen von t ordnet und den Faktor $N(\delta) = DE$ beiderseits forthebt:

$$(4) \qquad N\left(t - \frac{\delta_0}{\delta}\right) = t^n + \overline{C}_1 t^{n-1} + \overline{C}_2 t^{n-2} + \cdots,$$

worin $\overline{C}_1, \overline{C}_2 \ldots$ keinen anderen Nenner als E haben, und folglich ganze Funktionale in $\overline{Z}$ sind. Demnach ist nach der Definition § 179, 6. auch $\delta_0 : \delta$ ein ganzes Funktional, wie bewiesen werden sollte.

Demnach erhalten wir folgende Definitionen:

1. Das Funktional $\delta = \alpha x + \beta y + \cdots$ und jedes mit δ assoziierte Funktional ist der größte gemeinschaftliche Teiler von $\alpha, \beta, \ldots$

2. Ist $\alpha x + \beta y$ eine Einheit, so heißen α und β teilerfremd oder relativ prim. Gibt es Funktionale ξ, η, für die $\alpha \xi + \beta \eta$ eine Einheit ist, so sind α, β relativ prim.

3. Ist α relativ prim zu β und zu γ, so ist es auch relativ prim zu $\beta\gamma$.

Denn nach Voraussetzung sind

$$\varepsilon = \alpha x + \beta y, \quad \varepsilon_1 = \alpha u + \beta v$$

Einheiten (x, y, u, v neue Variablen).

$$\alpha(\alpha u x + \gamma v x + \beta u y) + \beta \gamma v y = \varepsilon \varepsilon_1,$$

also nach 3. α und $\beta\gamma$ relativ prim.

4. Ist α relativ prim zu β und $\alpha\mu$ durch β teilbar, so ist μ durch β teilbar.

Denn aus der Voraussetzung folgt:

$$\alpha \mu x + \beta \mu y = \varepsilon \mu,$$

woraus, da ε eine Einheit ist, sich der Beweis ergibt.

§ 182. Primfunktionale in $\overline{\Omega}$.

1. Definition. Ein ganzes Funktional π in $\overline{\Omega}$ heißt ein Primfunktional, wenn es keine Einheit ist und außer durch die Einheiten nur durch die mit ihm assoziierten Funktionale teilbar ist.

Daraus folgt:

2. Ist ein Produkt $\alpha\beta$ durch π teilbar, so ist wenigstens einer der beiden Faktoren, α oder β, durch π teilbar.

Denn ist weder α noch β durch π teilbar, so sind beide relativ prim zu π und nach § 181, 3. ist π auch relativ prim zu $\alpha\beta$.

3. Jedes von Null verschiedene ganze Funktional $\overline{\omega}$ ist durch ein Primfunktional teilbar.

Denn ist $\overline{\omega}$ nicht selbst ein Primfunktional, so ist es durch ein von ω verschiedenes Funktional α teilbar. Ist

$$\overline{\omega} = \alpha\overline{\omega}',$$

so ist $\overline{\omega}'$ keine Einheit und

$$N_a(\overline{\omega}) = N_a(\alpha) N_a(\overline{\omega}').$$

Die hier vorkommenden absoluten Normen sind ganze Funktionen in z und der Grad von $N_a(\overline{\omega}')$ ist kleiner als der Grad von $N_a(\omega)$. Ist $\overline{\omega}'$ noch kein Primfunktional, so kann man so fortfahren und muß schließlich auf einen Primfaktor π von $\overline{\omega}$ kommen.

In dieser Weise schließt man weiter wie in Bd. II, § 158, wobei nur an Stelle der dort benutzten Größe der ganzen rationalen Zahlen hier die Höhe des Grades ganzer rationaler Funktionen der Variablen z tritt. So erhält man auch die Sätze:

4. Jedes ganze Funktional $\overline{\omega}$ in $\overline{\Omega}$, das keine Einheit ist, läßt sich in eine endliche Anzahl von Primfaktoren zerlegen, und zwar nur auf eine Weise, wenn assoziierte Funktionale als nicht verschieden betrachtet werden.

Im folgenden müssen wir von dem Satz Gebrauch machen, daß eine ganze rationale Funktion von z mit numerischen Koeffizienten in lineare Faktoren zerlegbar ist, mit anderen Worten, wir müssen den Fundamentalsatz der Algebra von der Wurzelexistenz voraussetzen. Es folgt daraus zunächst:

5. Die ganze rationale Funktion von z niedrigsten Grades, die durch ein Primfunktional π teilbar ist, ist eine lineare Funktion $z - c$.

Nach § 180, 9. gibt es überhaupt ganz rationale Funktionen von z, die durch π teilbar sind. Zerlegt man eine solche Funk-

tion in lineare Faktoren, so muß nach 2. einer dieser Linearfaktoren durch π teilbar sein. Es können nicht zwei verschiedene Linearfunktionen $z - c$ und $z - c'$ durch dasselbe π teilbar sein, weil sonst die von Null verschiedene Konstante $c - c'$ durch π teilbar wäre.

6. Jede ganze Funktion ω in Ω ist nach dem Modul π mit einer Konstante b kongruent, d. h. man kann die Konstante b so wählen, das $\omega - b$ durch π teilbar wird.

Denn die Funktion ω genügt nach § 175 einer Gleichung:

$$\omega^n + a_1 \omega^{n-1} + \cdots + a_{n-1} \omega + a_n = 0,$$

worin die $a_1, \ldots, a_n$ ganze rationale Funktionen von z sind. Sind $a_1^0, \ldots, a_n^0$ die Reste dieser Funktionen bei der Teilung durch $z - c$, also Konstanten, so folgt:

$$\omega^n + a_1^0 \omega^{n-1} + \cdots + a_{n-1}^0 \omega + a_n^0 \equiv 0 \pmod{\pi},$$

und wenn man die Funktion auf der linken Seite in Linearfaktoren zerlegt:

(1) $$(\omega - b)(\omega - b')(\omega - b'') \cdots \equiv 0 \pmod{\pi}.$$

Es muß also wenigstens einer dieser Linearfaktoren durch π teilbar sein, was zu beweisen war.

Aus der nachgewiesenen einwertigen Zerlegbarkeit der Funktionale in Primfaktoren ergeben sich weitgehende Folgerungen, von denen die wichtigsten hier angeführt werden sollen.

Wenn in einem Funktional φ des Körpers Ω eine gewisse Anzahl der Hilfsvariablen, $x, y, \ldots$, nur im Zähler vorkommen, so möge

$$\varphi = \varphi(x, y, \ldots)$$

eine holomorphe Funktion von $x, y, \ldots$ heißen. Von denen gilt der Satz:

7. Eine holomorphe Funktion ist nur dann ein ganzes Funktional in Ω, wenn die Koeffizienten der geordneten Funktion φ ganze Funktionale sind.

Es genügt offenbar, den Satz für holomorphe Funktionen einer Variablen

(2) $$\varphi = x^m \varphi_0 + x^{m-1}\varphi_1 + \cdots + x \varphi_{m-1} + \varphi_m$$

nachzuweisen, weil er daraus durch vollständige Induktion allgemein bewiesen werden kann.

Dieser Beweis ergibt sich aber aus dem Gaussschen Satz:

Haben zwei holomorphe Funktionen

$$\alpha = \alpha_0 x^h + \alpha_1 x^{h-1} + \cdots + \alpha_h,$$
$$\beta = \beta_0 x^k + \beta_1 x^{k-1} + \cdots + \beta_k$$

ein Produkt

$$\gamma = \gamma_0 x^{h+k} + \gamma_1 x^{h+k-1} + \cdots + \gamma_{h+k},$$

dessen Koeffizienten ganze Funktionale sind, so können die γ_0, $\gamma_1, \ldots, \gamma_{h+k}$ nur dann alle durch ein Primfunktional π teilbar sein, wenn entweder alle $\alpha_0, \alpha_1, \ldots, \alpha_h$, oder alle $\beta_0, \beta_1, \ldots, \beta_k$ durch π teilbar sind, was ganz so bewiesen wird, wie in Bd. I, § 2.

Wenn nun (2) ein ganzes Funktional ist, ohne daß $\varphi_0, \varphi_1, \ldots, \varphi_m$ ganz sind, so kann man ein ganzes Funktional μ und darin einen Primfaktor π so bestimmen, daß

$$(3) \qquad \chi = \mu\varphi = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m,$$

durch π teilbar ist, $\alpha_0, \alpha_1, \ldots, \alpha_n$ aber nicht alle durch π teilbar sind.

Ist nun φ ganz, so genügt es einer Gleichung:

$$(4) \qquad E\varphi^m = a_1 E_1 \varphi^{m-1} + a_2 E_2 \varphi^{m-2} + \cdots + a_m E_m$$

und daraus durch Multiplikation mit μ^m:

$$(5) \qquad E\chi^m = \mu(a_1 E_1 \chi^{m-1} + a_2 E_2 \mu \chi^{m-2} + a_m E_m),$$

worin die $a_1, a_2, \ldots$ ganze Funktionen in Z, die $E, E_1, \ldots, E_m$ Einheiten in $\overline{Z}$ sind. Die Einheiten $E, E_1, \ldots, E_m$ können zwar x noch enthalten, können aber holomorph angenommen werden. Ordnen wir rechter Hand und linker Hand von (5) nach x, so sind die Koeffizienten von E nicht alle durch π teilbar. Ebenso sind nach dem erwähnten Satz die Koeffizienten von χ^m nicht alle durch π teilbar, während auf der rechten Seite alle Koeffizienten den Faktor μ, also auch den Faktor π haben. Das ist unmöglich und damit unser Satz bewiesen (Bd. II, § 159).

8. Ein holomorphes ganzes Funktional φ ist der größte gemeinschaftliche Teiler aller seiner Koeffizienten.

Sind $\alpha, \beta, \ldots$ die Koeffizienten von φ, so ist φ jedenfalls durch den größten gemeinschaftlichen Teiler von $\alpha, \beta, \ldots$ teilbar. Zerlegen wir eine Linearfunktion $z - c$ in ihre funktionalen Primfaktoren, so können wir in diesen Primfunktionalen π die Variablen beliebig bezeichnen, und da jedes Primfunktional in einem $z - c$ aufgehen muß, so können wir darin die Variablen von den Variablen $x, y, \ldots$ in φ verschieden annehmen. Demnach können

wir ein von den $x, y, \ldots$ freies, mit φ assoziiertes Funktional $\psi = \varepsilon \varphi$ bestimmen. Da dann φ / ψ ganz ist, so müssen nach 7. die Koeffizienten von φ alle durch ψ, und folglich auch alle durch φ teilbar sein. Was zu beweisen war.

Damit ist zugleich bewiesen:

9. Ein holomorphes ganzes Funktional geht in ein assoziiertes über, wenn die Variablen anders bezeichnet werden.

10. Jedes Funktional $\overline{\omega}$ in $\overline{\Omega}$ geht durch Multiplikation mit einer Einheit in $\overline{Z}$ in ein holomorphes Funktional über.

Denn man kann zunächst $\overline{\omega}$ als Quotienten zweier ganzer holomorpher Funktionale

$$\overline{\omega} = \frac{\psi}{\varphi}$$

darstellen. Setzt man $N(\varphi) = \varphi \varphi'$, so ist, wie die Formel (4) zeigt, in der $a_m E_m = \pm N(\varphi)$ ist, φ' mit einem holomorphen Funktional assoziiert, und es folgt:

$$E_m \overline{\omega} = \frac{\psi \varphi'}{a_m}. \tag{6}$$

11. Zu einem ganzen Funktional $\overline{\omega}$ kann man ein zweites μ so wählen, daß μ durch beliebig gegebene Primfunktionale $\pi_1, \pi_2, \ldots$ nicht teilbar wird, und daß

$$\overline{\omega} \mu = \alpha \tag{7}$$

eine Funktion in Ω wird.

Man stelle $\overline{\omega}$ nach 10. durch ein holomorphes Funktional φ dar. Dessen Koeffizienten sind nach 8. alle durch $\overline{\omega}$, aber nicht alle durch $\overline{\omega} \pi_1$ teilbar. Es gibt also eine Funktion α_1, die durch $\overline{\omega}$, aber nicht durch $\overline{\omega} \pi_1$ teilbar ist.

Nun setze man:

$$\overline{\omega}_1 = \overline{\omega} \pi_2 \pi_3 \ldots, \quad \overline{\omega}_2 = \overline{\omega} \pi_1 \pi_3 \ldots, \quad \overline{\omega}_3 = \overline{\omega} \pi_2 \pi_1 \ldots$$

und bestimme:

α_1 teilbar durch $\overline{\omega}_1$, nicht teilbar durch $\overline{\omega}_1 \pi_1$,
α_2 " " $\overline{\omega}_2$, " " " $\overline{\omega}_2 \pi_2$,
α_3 " " $\overline{\omega}_3$, " " " $\overline{\omega}_3 \pi_3$.
. . . .

Dann genügt

$$\alpha = \alpha_1 + \alpha_2 + \alpha_3 + \cdots$$

den Forderungen des Satzes 11.

12. **Jedes ganze Funktional $\overline{\omega}$ ist der größte gemeinschaftliche Teiler zweier Funktionen α, β in Ω.**

Um dies zu beweisen, nehmen wir $\alpha = \overline{\omega}\mu$, teilbar durch $\overline{\omega}$, dann β teilbar durch $\overline{\omega}$ und $\beta:\overline{\omega}$ relativ prim zu μ; dann ist

$$\overline{\omega} = \alpha x + \beta y$$

der größte gemeinschaftliche Teiler von α und β.

§ 183. Basen und Basisformen der Funktionale.

Es sei jetzt

$$\omega_1, \omega_2, \ldots, \omega_n \tag{1}$$

eine Minimalbasis des Körpers Ω (§ 176) und

$$\alpha_1, \alpha_2, \ldots, \alpha_n \tag{2}$$

eine andere Basis von Ω. Die lineare Substitution, durch die die α mit dem ω zusammenhängen, sei:

$$\alpha_s = \overset{i}{\Sigma} a_{s,i}\,\omega_i, \tag{3}$$

worin die $a_{s,i}$ ganze Funktionen in Z sind, deren Determinante

$$A = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{n,n} \tag{4}$$

nicht identisch verschwindet. Sind $t_1, t_2, \ldots, t_n$ Variable, so ist

$$\lambda = \alpha_1 t_1 + \alpha_2 t_2 + \cdots + \alpha_n t_n \tag{5}$$

der größte gemeinschaftliche Teiler von $\alpha_1, \alpha_2, \ldots, \alpha_n$.

Setzt man für $t_1, t_2, \ldots, t_n$ ganze Funktionen in Z, so entstehen aus λ ganze Funktionen in Ω, die alle durch λ teilbar sind.

1. **Man nennt λ eine Basisform und $\alpha_1, \alpha_2, \ldots, \alpha_n$ eine Basis des Funktionals λ, wenn man alle durch λ teilbaren Zahlen in Ω dadurch erhält, daß man für t_i ganze Funktionen in Z setzt.**

Bilden die α_i eine solche Basis, so kann man ganze Funktionen $g_{r,s}^{(i)}$ in Z, so bestimmen, daß

$$\alpha_r\, \omega_s = \overset{i}{\Sigma} g_{r,s}^{(i)}\, \alpha_i \tag{6}$$

wird.

Daraus folgt:

$$\lambda\, \omega_s = \overset{i}{\Sigma}\, \alpha_i\, t_{i,s}, \tag{7}$$

wenn

$$t_{i,s} = \overset{r}{\Sigma}\, g_{r,s}^{(i)}\, t_r \tag{8}$$

gesetzt ist, und indem man für α_i in (7) die Ausdrücke (3) substituiert:

(9) $$\lambda\,\omega_r = \sum^i \omega_i \sum^s a_{s,i}\, t_{s,r}.$$

Nach der Definition der Norm (§ 172) ist also $N(\lambda)$ die Determinante aus den Koeffizienten

$$\sum^s a_{s,i}\, t_{s,r},$$

und diese kann man nach dem Multiplikationssatz der Determinante in

(10) $$N(\lambda) = A\,T$$

zerlegen, worin A die Bedeutung (4) hat, und T die Determinante ist:

(11) $$T = \Sigma \pm t_{1,1}\, t_{2,2} \ldots t_{n,n}.$$

Hierin ist T eine homogene Funktion $n$ten Grades der t_i, deren Koeffizienten ganze Funktionen in Z sind. A ist selbst eine ganze Funktion in z. Man beweist nun wie in Bd. II, § 164, daß T eine Einheit ist. Wäre das nämlich nicht der Fall, so hätte T irgend einen Linearfaktor $z - c$, und man könnte nach einem elementaren Determinantensatz holomorphe ganze Funktionale y_i in z, die nicht alle durch $z - c$ teilbar sind, so bestimmen, daß

$$u_s = y_1\, t_{s1} + \cdots + y_n\, t_{sn}$$

durch $z - c$ teilbar wird (man kann den y_i sogar konstanten Koeffizienten geben, da man sie auf ihre Reste nach $z - c$ reduzieren kann).

Setzt man nun

$$\omega = \omega_1 y_1 + \omega_2 y_2 + \cdots + \omega_n y_n,$$

so folgt aus (7)

$$\lambda\,\omega = \alpha_1 u_1 + \alpha_2 u_2 + \cdots + \alpha_n u_n,$$

und daraus folgt, weil die α_i durch λ, die u_i durch $z - c$ teilbar sind, daß ω durch $z - c$ teilbar ist, was der Definition der Minimalbasis widerspricht. Demnach ergibt sich aus (10), daß A die absolute Norm des Funktionals λ ist:

(12) $$N_a(\lambda) = \Sigma \pm a_{11}\, a_{22} \ldots a_{nn}.$$

Für ein Primfunktional π können wir leicht eine Basis finden. Es können nicht alle Elemente $\omega_1, \omega_2, \ldots, \omega_n$ einer Minimalbasis durch π teilbar sein, weil ja durch die Linearform

(13) $$\omega = x_1\,\omega_1 + x_2\,\omega_2 + \cdots + x_n\,\omega_n$$

auch die Funktion „1“ darstellbar sein muß. Nehmen wir an, ω_1 sei nicht durch π teilbar. Nach § 182, 6. gibt es Konstanten $c_1, c_2, \ldots, c_n$, deren erste unbeschadet der Allgemeinheit $= 1$ angenommen werden kann, die den Bedingungen:

$$\omega_1 \equiv 1, \quad \omega_2 \equiv c_2, \quad \ldots, \quad \omega_n = c_n \pmod{\pi}$$

genügen. Wir setzen:

$$\begin{aligned} \alpha_1 &= (z - c)\,\omega_1, \\ \alpha_2 &= \omega_2 - c_2\,\omega_1, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \alpha_n &= \omega_n - c_n\,\omega_1. \end{aligned} \tag{14}$$

Daß dies eine Basis von π ist, ersieht man sofort, wenn man die Funktion (13) so darstellt:

$$\omega = x_2\,\alpha_2 + \cdots + x_n\,\alpha_n + (x_1 + c_2\,x_2 + \cdots + c_n\,x_n)\,\omega_1; \tag{15}$$

da $\alpha_2, \ldots, \alpha_n$ durch π teilbar sind, so kann ω nur dann durch π teilbar sein, wenn die ganze Funktion in Z:

$$x_1 + c_2\,x_2 + \cdots + c_n\,x_n$$

durch $(z - c)$ teilbar und folglich ω durch die Formel (5) darstellbar ist. Hiernach ergeben die Formeln (10) und (14):

$$N_a(\pi) = z - c, \tag{16}$$

also den Satz:

2. Die absolute Norm eines Primfunktionals ist eine lineare Funktion von z.

Dieser Satz bedeutet einen wesentlichen Unterschied zwischen den Theorien der Zahlen und der Funktionen. In der Zahlentheorie gibt es Primideale verschiedener Grade, deren Norm eine Potenz einer Primzahl ist. In der Theorie der Funktionen haben wir nur Primfunktionale ersten Grades. Dies rührt daher, daß wir vermöge des Fundamentalsatzes der Algebra jede ganze Funktion einer Variablen nach dem Modul π in lineare Faktoren zerlegen können.

Die Zahl der Primfaktoren, in die $(z - c)$ zerfällt, ist hiernach n, da $N(z - c) = (z - c)^n$ ist.

Fassen wir die untereinander gleichen Primfaktoren in Potenzen zusammen, so ist

$$z - c = \varepsilon\,\pi_1^{e_1}\,\pi_2^{e_2}\,\pi_3^{e_3} \ldots, \tag{17}$$

worin

$$n = e_1 + e_2 + e_3 + \cdots, \tag{18}$$

wo ε eine Einheit ist.

§ 184. Basisform und Verzweigungsfunktional.

Unter der Basisform des Körpers Ω wollen wir die Linearform verstehen:

(1) $$\tau = \omega_1 t_1 + \omega_2 t_2 + \cdots + \omega_n t_n,$$

in der $t_1, t_2, \ldots, t_n$ die Funktionalvariablen sind, und deren Koeffizienten $\omega_1, \omega_2, \ldots, \omega_n$ eine Minimalbasis von Ω bilden. Diese Form ist der größte gemeinschaftliche Teiler von $\omega_1, \omega_2, \ldots, \omega_n$ und folglich eine Einheit. Aus τ kann man alle ganzen Funktionen in Ω ableiten, indem man für die Variablen $t_1, t_2, \ldots, t_n$ ganze Funktionen in Z setzt.

Setzen wir

(2) $$F(t) = N(t - \tau) = t^n + A_1 t^{n-1} + \cdots + A_{n-1} t + A_n,$$

so sind die $A_1, A_2, \ldots, A_n$ holomorphe ganze Funktionale in Z, und τ genügt der Gleichung $n$ten Grades:

(3) $$F(\tau) = 0.$$

Ist π ein Primfunktional und

$$N_a(\pi) = z - c,$$

so kann man nach § 182, 6. die Konstanten $c_1, c_2, \ldots, c_n$ aus den Kongruenzen

(4) $$\omega_1 \equiv c_1, \ \omega_2 \equiv c_2, \ldots, \omega_n \equiv c_n \pmod{\pi}$$

bestimmen, und wenn man

(5) $$\tau_0 = c_1 t_1 + c_2 t_2 + \cdots + c_n t_n$$

setzt, so ist τ_0 ein konstantes Funktional, und $\tau - \tau_0$ ist durch π teilbar. Es ist nun zu beweisen:

> 3. Das Primfunktional π ist der größte gemeinschaftliche Teiler von $\tau - \tau_0$ und $z - c$:
>
> (6) $$\pi = u(\tau - \tau_0) + v(z - c),$$
>
> und wenn daher $(z - c)$ durch eine höhere als die erste Potenz von π teilbar ist, so ist $\tau - \tau_0$ nur durch die erste Potenz von π teilbar.

Zunächst ergibt sich aus der Definition § 181, daß

(7) $$\tau - \tau_0 = t_1(\omega_1 - c_1) + t_2(\omega_2 - c_2) + \cdots + t_n(\omega_n - c_n)$$

der größte gemeinschaftliche Teiler von $(\omega_1 - c_1), (\omega_2 - c_2), \ldots, (\omega_n - c_n)$ ist. Ist nun

(8) $$\omega = x_1 \omega_1 + x_2 \omega_2 + \cdots x_n \omega_n \equiv 0 \pmod{\pi},$$

so ist $x_1 c_1 + x_2 c_2 + \cdots + x_n c_n$ durch π, und weil es eine Funktion in Z ist, durch $(z - c)$ teilbar. Wir setzen:

$$x_1 c_1 + x_2 c_2 + \cdots + x_n c_n = (z - c) y$$

und erhalten aus (8)

$$(9) \quad \omega = x_1(\omega_1 - c_1) + x_2(\omega_2 - c_2) + \cdots + x_n(\omega_n - c_n) + (z - c) y$$
$$= (\tau - \tau_0) + (z - c) y.$$

Hätte nun $(\tau - \tau_0)$ und $(z - c)$ den gemeinschaftlichen Teiler $\pi\delta$, so könnte man nach § 182, 11. eine durch π teilbare, zu δ teilerfremde Funktion ω in Ω finden. Dem widerspricht aber die Gleichung (9), und damit ist unser Satz bewiesen.

Es sei

$$(10) \quad \Phi(t) = B_0 t^m + B_1 t^{m-1} + \cdots + B_{m-1} t + B_m$$

eine Funktion $m$ten Grades von t, und $B_0, B_1, \ldots, B_m$ seien ganze holomorphe Funktionale in $\bar{Z}$ mit den Funktionalvariablen $t_1, t_2, \ldots, t_n$, die der Kongruenzbedingung

$$(11) \quad \Phi(\tau) \equiv 0 \pmod{z - c}$$

genügt [wie z. B. die Funktion $F(t) = N(t - \tau)$]. Dann ist

$$\Phi(\tau_0) \equiv 0 \pmod{\pi},$$

und wenn wir $\Phi(t)$ durch $\tau - \tau_0$ dividieren, so ergibt sich

$$(12) \quad \Phi(t) \equiv (t - \tau_0)\Phi_1(t) \pmod{\pi},$$

worin $\Phi_1(t)$ ein holomorphes ganzes Funktional in $\bar{Z}$ ist (weil τ_0 als **konstantes** Funktional in $\bar{Z}$ enthalten ist). Da nun in (12) außer den Funktionalvariablen nur rationale Funktionen von z vorkommen, so muß diese Kongruenz auch für den Modul $z - c$ gültig sein:

$$(13) \quad \Phi(t) \equiv (t - \tau_0)\Phi_1(t) \pmod{z - c}.$$

Ist π' ein zweites Primfunktional, das auch mit π identisch sein kann, und $z - c$ durch $\pi\pi'$ teilbar, und $\tau \equiv \tau'_0 \pmod{\pi'}$, so ist $(\tau - \tau_0) : \pi$ relativ prim zu π' (nach 3.) und wegen (11) ist $\Phi_1(\tau'_0) \equiv 0 \pmod{\pi'}$. Daraus schließt man

$$\Phi_1(t) \equiv (t - \tau'_0)\Phi_2(t)$$

zunächst für den Modul π', dann aber auch, da die Funktionale in $\bar{Z}$ liegen, auch für den Modul $(z - c)$. Wir haben also:

$$(14) \quad \Phi(t) \equiv (t - \tau_0)(t - \tau'_0)\Phi_2(t) \pmod{z - c}.$$

Daraus schließen wir auf folgenden wichtigen Satz:

4. **Es sei nach** § 183, (17)

$$(15) \quad z - c = \pi_1 \pi_2 \ldots \pi_n$$

in n (gleiche oder verschiedene) Primfaktoren zerlegt, und

(16) $$\tau_1, \tau_2, \ldots, \tau_n$$

seien die konstanten Funktionale, denen τ nach den Modulen

(17) $$\pi_1, \pi_2, \ldots, \pi_n$$

kongruent wird.

Es sei $\Phi(t)$ ein ganzes holomorphes Funktional in z vom Grade m in bezug auf t, das der Bedingung

(18) $$\Phi(\tau) \equiv 0 \pmod{z - c}$$

genügt. Dann ist:

(19) $$\Phi(t) \equiv (t - \tau_1)(t - \tau_2) \ldots (t - \tau_n)\Psi(t) \pmod{z - c},$$

worin Ψ ein ebensolches Funktional vom Grade $m - n$ ist.

Es folgt daraus:

5. Ein Funktional Φ, das der Bedingung (18) genügt, kann nicht von niedrigerem als $n$tem Grade sein.

Und auf die Funktion $F(t)$ angewandt, folgt die Formel:

(20) $$F(t) = N(t - \tau) \equiv (t - \tau_1)(t - \tau_2) \ldots (t - \tau_n) \pmod{z - c}.$$

Die Kongruenz (20) können wir in folgender Weise durch eine Gleichung ersetzen:

Wir fassen, wie in (17) des vorigen Paragraphen, in der Zerlegung von $z - c$ in Primfaktoren die gleichen Faktoren zusammen und setzen:

(21) $$z - c = \pi_1^{e_1} \pi_2^{e_2} \ldots \pi_m^{e_m}$$
$$e_1 + e_2 + \cdots + e_m = n,$$

dann ist nach (20):

(22) $$F(t) = (t - \tau_1)^{e_1}(t - \tau_2)^{e_2} \ldots (t - \tau_m)^{e_m} + (z - c)R(t),$$

worin $R(t)$ ein ganzes Funktional zunächst in Ω ist. Die Formel (22) selbst sagt aber, daß $R(t)$ in $\overline{Z}$ enthalten ist, und daß es eine ganze Funktion der Funktionalvariablen $t, t_1, t_2, \ldots, t_n$ ist.

Wir können also auch die Ableitung der Gleichung (12) in bezug auf t bilden und erhalten:

(23) $$\begin{aligned} F'(t) = {} & e_1(t - \tau_1)^{e_1 - 1}(t - \tau_2)^{e_2} \ldots (t - \tau_m)^{e_m} \\ & + e_2(t - \tau_1)^{e_1}(t - \tau_2)^{e_2 - 1} \ldots (t - \tau_m)^{e_m} \\ & \ldots \ldots \ldots \ldots \ldots \\ & + e_m(t - \tau_2)^{e_1}(t - \tau_2)^{e_2} \ldots (t - \tau_m)^{e_m - 1} + (z - c)R'(t) \end{aligned}$$

und hierin liegt der Beweis des folgenden Hauptsatzes, den man erhält, wenn man $t = \tau_1$ setzt.

6. Wenn $e_1 = 1$ ist, so ist $F'(\tau)$ nicht durch π_1 teilbar. Sonst ist $F'(\tau)$ durch $\pi_1^{e_1-1}$, aber nicht durch $\pi_1^{e_1}$ teilbar. Das Gleiche gilt von den übrigen Primfaktoren von $(z - c)$ und folglich ist $F'(\tau)$ teilerfremd zu allen Primfaktoren $z - c$ in Z, die nicht durch das Quadrat eines Primfaktors in Ω teilbar sind.

Es gibt also nur eine endliche Anzahl von Primfaktoren $(z - c)$, die durch eine höhere als die erste Potenz eines Primfaktors in Ω teilbar sind, und $F'(\tau)$ ist, in Primfaktoren zerlegt, das Produkt aller Faktoren π^{e-1}, wenn π^e die höchste in $N(\pi) = z - c$ aufgehende Potenz von π ist.

Das Funktional $F'(\tau)$ wird das Verzweigungsfunktional des Körpers Ω genannt.

Für die absolute Norm des Verzweigungsfunktionals erhalten wir:

$$N_a F'(\tau) = \Pi(z - c)^{e_1 - 1 + e_2 - 1 + \cdots}, \tag{24}$$

worin sich das Produkt Π auf alle Linearfaktoren $(z - c)$ erstreckt, die durch eine höhere als die erste Potenz eines Primfaktors teilbar sind.

Wir können noch zeigen, daß diese absolute Norm nichts anderes ist, als die Körperdiskriminante D.

Um dies zu beweisen, setzen wir:

$$\tau^k = u_{k,1}\omega_1 + u_{k,2}\omega_2 + \cdots + u_{k,n}\omega_n, \tag{25}$$

worin die $u_{k,1}, u_{k,2}, \ldots, u_{k,n}$ homogene Funktionen $k$ten Grades von $t_1, t_2, \ldots, t_n$ sind, und die Determinante

$$U = \begin{vmatrix} u_{1,0}, & u_{2,0}, & \ldots, & u_{n,0} \\ u_{1,1}, & u_{2,1}, & \ldots, & u_{n,1} \\ \cdot & \cdot & \cdot & \cdot \\ u_{1,n-1}, & u_{2,n-1}, & \ldots, & u_{n,n-1} \end{vmatrix} \tag{26}$$

ist eine Einheit.

Denn wäre U keine Einheit, so hätte sie wenigstens einen Linearfaktor $z - c$, und man könnte die ganzen rationalen holomorphen Funktionale $y_0, y_1, \ldots, y_{n-1}$ so bestimmen, daß

$$u_{r,0}y_0 + u_{r,1}y_1 + \cdots + u_{r,n-1}y_{n-1} \equiv 0 \pmod{z - c}$$

wäre, ohne daß alle y_s durch $z - c$ teilbar sind.

Dann würde sich aus (20) eine Kongruenz ergeben:

$$y_0 + y_1\tau + y_2\tau^2 + \cdots + y_{n-1}\tau^{n-1} \equiv 0 \pmod{z - c},$$

was nach dem Satz 5. nicht möglich ist.

Nach § 174, (17) und § 176, (9) ist

$$\begin{aligned} NF'(\tau) &= \pm\Delta(1, \tau, \tau^2, \ldots, \tau^{n-1}) \\ &= \pm U^2\Delta(\omega_1, \omega_2, \ldots, \omega_n) \\ &= \pm U^2\Delta; \end{aligned} \tag{27}$$

also ist

$$N_a F'(\tau) = \Delta \tag{28}$$

die Körperdiskriminante, die hiernach durch (24) in lineare Faktoren zerlegt ist.

Die gewonnenen Resultate benutzen wir noch zum Beweis des folgenden Satzes:

7. Ist eine ganze Funktion in Ω

$$\omega = x_1\omega_1 + x_2\omega_2 + \cdots + x_n\omega_n \tag{29}$$

durch jedes in $z - c$ aufgehende Primfunktional teilbar, so ist $S(\omega)$ durch $z - c$ teilbar.

Die $x_1, x_2, \ldots, x_n$ sind hier ganze Funktionen in Z. Die Funktion ω geht aus τ hervor durch die Substitution

$$t_1 = x_1,\ t_2 = x_2,\ \ldots,\ t_n = x_n. \tag{30}$$

Ist also ω durch π teilbar, und $\omega_1 \equiv c_1, \ldots, \omega_n \equiv c_n \pmod{\pi}$, so ist

$$x_1c_1 + x_2c_2 + \cdots + x_nc_n \equiv 0 \pmod{\pi}$$

und folglich auch, als Funktion in Z, durch $z - c$ teilbar. Sind also $\tau_1, \tau_2, \ldots, \tau_m$ die konstanten Funktionale, denen τ nach den Primfaktoren $\pi_1, \pi_2, \ldots, \pi_m$ von $(z - c)$ kongruent ist, und gehen diese durch die Substitution (30) in $\tau_1^0, \tau_2^0, \ldots, \tau_m^0$ über, so sind alle diese Funktionen durch $(z - c)$ teilbar [weil sie n. V. durch einen Primteiler von $(z - c)$ teilbar sind]. Nun ist nach (22)

$$-S(\tau) \equiv e_1\tau_1 + e_2\tau_2 + \cdots + e_m\tau_m, \tag{31}$$

und mithin

$$-S(\omega) \equiv e_1\tau_1^0 + e_2\tau_2^0 + \cdots + e_m\tau_m^0 \equiv 0 \pmod{z - c},$$

wie zu beweisen war.

§ 185. Die gebrochenen Funktionen in Ω und die Taylorsche Entwickelung.

Eine gebrochene Funktion η im Körper Ω kann auf unendlich viele Arten durch Multiplikation mit einer ganzen Funktion ν in eine ganze Funktion μ verwandelt werden. Es ist dann

(1) $$\eta = \frac{\mu}{\nu},$$

und μ heißt der Zähler, ν der Nenner von η. Diese beiden Funktionen sind durch η nicht vollständig bestimmt, wohl aber sind die Funktionale bestimmt, die übrig bleiben, wenn alle gemeinschaftlichen Funktionalfaktoren im Zähler und Nenner herausgehoben werden. Denn ist

(2) $$\frac{\mu}{\nu} = \frac{\mu'}{\nu'}; \quad \mu\nu' = \nu\mu',$$

so muß jedes Primfunktional, das in ν, aber nicht in μ aufgeht, in ν' aufgehen. Die so aus η bestimmten Funktionale $\overline{\alpha}$ und $\overline{\beta}$ nennen wir Zählerfunktional und Nennerfunktional von η. Um η durch Funktionen darzustellen, nehme man zunächst eine Funktion ν, teilbar durch $\overline{\beta}$, aber sonst beliebig und setze $\nu = \overline{\beta}\,\overline{\gamma}$; darin kann $\overline{\gamma}$ relativ prim zu einem beliebigen Funktional angenommen werden. Dann ist $\eta\nu$ eine durch $\overline{\gamma}$ teilbare ganze Funktion, und man setze

$$\eta\,\nu = \mu = \overline{\alpha}\,\overline{\gamma}.$$

Das Funktional $\overline{\alpha}$ kann aber, wie wir später noch nachweisen werden, bei gegebenem $\overline{\beta}$ nicht mehr beliebig sein.

Die Funktionale $\overline{\alpha}, \overline{\beta}$ werden wir auch kurz den Zähler und den Nenner von η nennen.

Ist π ein Primfunktional, so gibt es Zahlen (Konstanten) a, b, a', b', die den Kongruenzen

$$\mu \equiv a, \quad \nu \equiv b, \quad \mu' \equiv a', \quad \nu' \equiv b' \pmod{\pi}$$

genügen, und aus (2) folgt

$$a\,b' = b\,a', \quad \frac{a}{b} = \frac{a'}{b'} = c,$$

vorausgesetzt, daß ν und ν' nicht durch π teilbar sind. Es ist dann $\eta - c$ eine Funktion in Ω, in der der Zähler, aber nicht der Nenner durch π teilbar ist. Ist ϱ eine ganze oder gebrochene Funktion, in der der Zähler durch π, aber nicht durch π^2, der Nenner auch nicht durch π teilbar ist, so ist $(\eta - c) : \varrho$ eine Funktion, deren Nenner nicht durch π teilbar ist und deren Zähler den Faktor π einmal weniger enthält als $(\eta - c)$. Wir setzen:

$$\eta - c = \varrho\,\eta_1.$$

Dieselbe Betrachtung wenden wir auf η_1 an und bekommen so eine beliebig fortzusetzende Reihe von Gleichungen:

$$\begin{aligned} \eta &= c + \varrho\,\eta_1, \\ \eta_1 &= c_1 + \varrho\,\eta_2, \\ &\cdots\cdots \\ \eta_{r-1} &= c_{r-1} + \varrho\,\eta_r, \end{aligned} \tag{3}$$

woraus sich ergibt:

$$\eta = c + c_1\varrho + c_2\varrho^2 + \cdots + c_{r-1}\varrho^{r-1} + \eta_r\varrho^r. \tag{4}$$

Die Reihe der Konstanten $c, c_1, c_2, \ldots, c_{r-1}$ ist durch η vollständig bestimmt und $\eta_1, \eta_2, \ldots, \eta_r$ ist eine Reihe von Funktionen in Ω, deren Nenner nicht durch π teilbar ist.

Man könnte diesen Ausdruck die Taylorsche Entwickelung der Funktion η nach Potenzen von ϱ nennen. Eine ähnliche Entwickelung läßt sich auch für eine Funktion η geben, deren Nenner durch π teilbar ist, nur daß dabei auch negative Potenzen auftreten: Man kann nämlich eine Potenz ϱ^s so bestimmen, daß der Nenner von $\varrho^s\eta$ nicht mehr durch π teilbar ist, und wenn man auf dieses Produkt die Entwickelung (4) anwendet, so folgt:

$$\eta = c\varrho^{-s} + c_1\varrho^{-s+1} + \cdots + c_{r-1}\varrho^{r-s-1} + \eta_r\varrho^{r-s}. \tag{5}$$

§ 186. Birationale Transformation.

Wir kommen jetzt zu einem Gegenstand, der das Gebiet der algebraischen Funktionen vorzugsweise von dem der algebraischen Zahlen unterscheidet, und der Grund dafür ist, daß die Theorie der ganzen Funktionen und Funktionale für die Funktionen bei weitem nicht den Charakter der Invarianz hat, wie bei den Zahlen; das ist die birationale Transformation.

Ist z_1 irgend eine nicht konstante Funktion des Körpers Ω und $N(t - z_1)$ die $f$te Potenz einer irreduziblen Funktion $e$ten Grades (§ 172, 6.), so besteht zwischen z und z_1 eine Gleichung, die in bezug auf z_1 vom $e$ten Grade ist, deren Grad in bezug auf z, wenn Nenner und überflüssige Faktoren weggeschafft sind, mit e_1 bezeichnet werde. Diese Gleichung sei

$$G(\overset{e}{z_1}, \overset{e_1}{z}) = 0. \tag{1}$$

Unter den verschiedenen Gleichungen dieser Form gibt es nur eine irreduzible und diese ist sowohl in bezug auf z als in bezug auf z_1 von möglichst niedrigem Grade (Bd. I, § 20).

Ist θ eine primitive Funktion des Körpers Ω, so ist nach § 172, (12)

$$z_1^h\,\theta^k \quad \begin{matrix} h = 0, 1, \ldots, e-1 \\ k = 0, 1, \ldots, f-1 \end{matrix} \tag{2}$$

eine Basis des Körpers Ω, und folglich kann jede Funktion ω in Ω in der Form dargestellt werden:

(3) $$\omega = \xi_0 + \xi_1 \theta + \cdots + \xi_{f-1} \theta^{f-1},$$

worin die $\xi_0, \xi_1, \ldots, \xi_{f-1}$ rationale Funktionen von z und z_1 sind, also Zahlen des durch (1) bestimmten Körpers. Setzen wir

(4) $$n = e f, \quad n_1 = e_1 f,$$

so lassen sich die Funktionen ξ_i in jeder der beiden Formen darstellen:

(5) $$\begin{aligned} \xi &= x_0 + x_1 z_1 + x_2 z^2 + \cdots + x_{e-1} z_1^{e-1}, \\ &= y_0 + y_1 z + y_2 z^2 + \cdots + y_{e_1-1} z^{e_1-1}, \end{aligned}$$

worin die x rationale Funktionen von z, die y rationale Funktionen von z_1 sind.

1. Demnach läßt sich jede Funktion ω linear mit rationalen Koeffizienten in z_1 darstellen durch die n_1-Funktionen:

(6) $$z^r \theta^s \quad \begin{matrix} r = 0, 1, \ldots, e_1 - 1 \\ s = 0, 1, \ldots, f - 1 \end{matrix},$$

die wir in irgend einer Reihenfolge mit

(7) $$\eta_1, \eta_2, \ldots, \eta_{n_1}$$

bezeichnen, und diese Funktionen sind linear unabhängig, d. h. es besteht zwischen ihnen keine lineare Relation mit rationalen Koeffizienten in z_1:

$$x_1 \eta_1 + x_2 \eta_2 + \cdots + x_{n_1} \eta_{n_1} = 0,$$

außer wenn die $x_1, x_2, \ldots, x_{n_1}$ alle verschwinden.

Denn f ist der niedrigste Grad einer Gleichung für θ mit rationalen Koeffizienten in z und z_1 (§ 172).

Betrachten wir nun das Funktional

(8) $$\tau_1 = t_1 \eta_1 + t_2 \eta_2 + \cdots + t_{n_1} \eta_{n_1}$$

mit den Funktionalvariablen $t_1, t_2, \ldots, t_{n_1}$, so ergibt sich ein System von Gleichungen:

(9) $$\tau_1^r = x_{1,r} \eta_1 + x_{2,r} \eta_2 + \cdots + x_{n_1,r} \eta_{n_1},$$

worin r jede natürliche Zahl, auch 0, sein kann, und die $x_{i,r}$ rationale holomorphe Funktionale in z_1 sind. Es ergibt sich daraus durch Elimination der η eine Gleichung

(10) $$\Phi(\tau_1) = \tau_1^m + A_1 \tau_1^{m-1} + \cdots + A_{m-1} \tau_1 + A_m = 0$$

höchstens vom Grade n_1 mit rationalen Funktionalen in z_1 als Koeffizienten.

Es ist zu beweisen, daß dieser Grad nicht kleiner als n_1 sein kann, oder was damit gleichbedeutend ist, daß die $\eta_1, \eta_2, \ldots, \eta_{n_1}$ rational durch τ_1 darstellbar sind. Dies ergibt sich, wenn man (10) nach einem der t_ν partiell differentiiert:

$$\Phi'(\tau_1)\,\eta_\nu + \frac{\partial A_1}{\partial t_\nu}\,\tau_1^{m-1} + \cdots + \frac{\partial A_{m-1}}{\partial t_\nu}\,\tau_1 + \frac{\partial A_m}{\partial t_\nu} = 0.$$

Da nun $\Phi'(\tau_1)$ nicht verschwindet, wenn m der möglichst niedrige Grad der Gleichung (10) ist, so erhält man daraus unmittelbar die gesuchte Darstellung von η_ν. Also muß $m = n_1$ sein. Damit ist bewiesen:

2. Das Funktional τ_1 genügt einer irreduziblen Gleichung $n_1$ten Grades in z_1.

Setzen wir also in (9) $r = 0, 1, 2, \ldots, n_1 - 1$, so ergibt sich ein System linearer Gleichungen für $\eta_1, \eta_2, \ldots, \eta_{n_1}$, deren Determinante ein nicht verschwindendes Funktional in z_1 ist, und man kann also für die Variable t_i solche konstante Werte setzen, daß die Determinante auch dann nicht verschwindet. Geht τ_1 durch diese Substitution in θ_1 über, so kann man aus dem System (9) die $\eta_1, \eta_2, \ldots, \eta_{n_1}$ rational durch z_1 und θ_1 ausdrücken.

Damit ist aber bewiesen:

3. Ist z_1 eine beliebige, nicht konstante Funktion in Ω, und θ_1 eine zweite Funktion desselben Körpers, die keiner Gleichung von niedrigerem als $n_1$ten Grade in z_1 genügt, so sind alle Funktionen des Körpers Ω, also auch z und θ, rational durch z_1 und θ_1 ausdrückbar.

Zwischen irgend zwei Funktionen α, β des Körpers Ω besteht immer eine Gleichung mit konstanten Koeffizienten

$$F(\alpha, \beta) = 0, \tag{11}$$

und unter allen möglichen Gleichungen dieser Form ist eine von möglichst niedrigem Grade, sowohl in bezug auf α als in bezug auf β.

Sechsundzwanzigster Abschnitt.

Zahlenwerte der algebraischen Funktionen.

§ 187. Der Punkt.

Es entsteht nun die Frage, wie man den algebraischen Funktionen eine Bedeutung im Gebiete der Zahlen beilegen kann. Wir setzen dabei das Gebiet der reellen und imaginären rationalen und irrationalen Zahlen als gegeben voraus, und in diesem Gebiete das Rechnen mit den vier Spezies. Wir erweitern dieses Gebiet durch Hinzufügung eines Zahlzeichens „Unendlich“: ∞, und rechnen auch mit diesem Zeichen in bekannter Weise, so daß

(1) $$\frac{1}{\infty} = 0, \quad \frac{1}{0} = \infty, \quad \infty \cdot \infty = \infty$$

ist, während den Symbolen

$$\infty \pm \infty, \quad 0 \cdot \infty, \quad \frac{0}{0}, \quad \frac{\infty}{\infty}$$

keine Bedeutung zukommt (oder auch, in jedem einzelnen Falle nach Bedarf, ein beliebiger Zahlwert beigelegt wird).

Der Körper Ω besteht jetzt aus allen möglichen algebraischen Funktionen $\alpha, \beta, \gamma, \ldots$, die nach § 186 als rationale Funktionen von zweien unter ihnen mit Zahlenkoeffizienten dargestellt werden können. Auf die Art dieser Darstellung kommt es zunächst nicht an.

Wir stellen nun folgende Definition auf:

1. Wenn alle Individuen $\alpha, \beta, \gamma, \ldots$ des Körpers Ω durch bestimmte Zahlwerte $\alpha_0, \beta_0, \gamma_0, \ldots$ in der Weise ersetzt werden, daß

1. $\alpha = \alpha_0$, wenn α konstant,
2. $(\alpha + \beta)_0 = \alpha_0 + \beta_0$,
3. $(\alpha - \beta)_0 = \alpha_0 - \beta_0$,
4. $(\alpha\beta)_0 = \alpha_0 \beta_0$,
5. $\left(\frac{\alpha}{\beta}\right)_0 = \frac{\alpha_0}{\beta_0}$,

so ordnen wir einem solchen Zusammentreffen von Werten einen Punkt $\mathfrak{P}$ zu. Wir sagen: $\alpha = \alpha_0$, oder α hat den Wert α_0 im Punkte $\mathfrak{P}$. Zwei Punkte $\mathfrak{P}$ und $\mathfrak{P}'$ heißen dann und nur dann verschieden, wenn es wenigstens eine Funktion in Ω gibt, die in $\mathfrak{P}$ und $\mathfrak{P}'$ verschiedene Werte hat.

Die Regeln 2. bis 5. versagen in den Ausnahmefällen, nämlich 2. und 3., wenn α_0 und $\beta_0 = \infty$ sind; 4., wenn $\alpha_0 = 0$, $\beta_0 = \infty$ oder $\alpha_0 = \infty$, $\beta_0 = 0$ wird, und 5., wenn α_0 und β_0 beide $= 0$ oder beide $= \infty$ sind.

Trotzdem müssen die Funktionen $(\alpha \pm \beta)_0$, $(\alpha\beta)_0$ und $(\alpha : \beta)_0$ auch in diesen Fällen bestimmte Werte haben, die aber nicht unmittelbar aus den Vorschriften 2. bis 5., sondern auf indirektem Wege bestimmt werden.

Der Punkt ist hiernach ein zu dem Körper Ω gehöriger invarianter Begriff, der nichts mit dem zufälligen Umstand zu tun hat, welche der Funktionen von Ω wir als die unabhängige Variable betrachten.

Um alle Punkte zu finden, verfahre man so: Ist $\mathfrak{P}$ ein Punkt, so gibt es Funktionen, die in ihm einen endlichen Wert haben, denn wenn eine Funktion α in $\mathfrak{P}$ unendlich ist, so ist $1 : \alpha$ endlich. Eine solche Funktion nehme man als unabhängige Variable z und bezeichne ihren Wert im Punkt $\mathfrak{P}$ mit c. Alle ganzen Funktionen von z sind dann gleichfalls in $\mathfrak{P}$ endlich, denn ist ω eine ganze Funktion, die der Gleichung

$$\omega^n + a_1 \omega^{n-1} + \cdots + a_n = 0$$

genügt, so muß

$$1 + \frac{a_1}{\omega} + \frac{a_2}{\omega^2} + \cdots + \frac{a_n}{\omega^n} = 0$$

in $\mathfrak{P}$ befriedigt sein, und da die $a_1, a_2, \ldots, a_n$ als ganze rationale Funktionen von z in $\mathfrak{P}$ endlich sind, so kann ω nicht $= \infty$ sein.

Jede Kongruenz nach dem Modul $z - c$ muß daher im Punkt $\mathfrak{P}$ in eine richtige Gleichung übergehen, auch wenn diese Kongruenz zwischen holomorphen ganzen Funktionalen besteht. Ist also τ die Basisform von Ω in Z, so muß nach § 184, (20) die Gleichung bestehen:

$$(\tau - \tau_1)(\tau - \tau_2) \ldots (\tau - \tau_n) = 0.$$

Es muß also einer der Faktoren der linken Seite in $\mathfrak{P}$ verschwinden. Ist dies $\tau - \tau_1$, so entspricht diesem Faktor ein Primfaktor π von $z - c$. Es wird also in $\mathfrak{P}$

(2) $$\omega_1 = c_1,\ \omega_2 = c_2, \ldots, \omega_n = c_n,$$

wenn $c_1, c_2, \ldots, c_n$ die durch die Kongruenzen

(3) $$\omega_1 \equiv c_1,\ \omega_2 \equiv c_2,\ \ldots,\ \omega_n \equiv c_n \pmod{\pi}$$

bestimmten Zahlwerte sind. Hierdurch sind die Werte aller ganzen Funktionen von z im Punkt $\mathfrak{P}$ bestimmt. Jede ganze Funktion ω ist nach dem Modul $z - c$ einem Ausdruck

$$a_1 \omega_1 + a_2 \omega_2 + \cdots + a_n \omega_n$$

mit konstantem Koeffizienten a kongruent und ist dann und nur dann durch π teilbar, wenn

$$a_1 c_1 + a_2 c_2 + \cdots + a_n c_n = 0$$

ist. Demnach folgt:

2. Unter den ganzen Funktionen von z haben nur die durch π teilbaren in $\mathfrak{P}$ den Wert 0.

Da man jede gebrochene Funktion in Ω so darstellen kann, daß Zähler und Nenner nicht zugleich durch π teilbar sind, so ist hierdurch der Wert einer jeden Funktion in $\mathfrak{P}$ bestimmt.

3. Der Primfaktor π heißt durch den Punkt $\mathfrak{P}$ erzeugt. Er kann nicht durch einen von $\mathfrak{P}$ verschiedenen Punkt erzeugt werden.

Man kann auch umgekehrt aus jedem Primfaktor π in z einen Punkt erzeugen.

Ist $z - c$ die durch π teilbare Linearfunktion, so gebe man der Funktion z den Wert c. Dann nehme man eine durch π, aber nicht durch π^2 teilbare Funktion ϱ und setze nach § 185, (5) für jede Funktion η:

(4) $$\eta = a\varrho^m + \eta_1 \varrho^{m+1},$$

worin m eine ganze rationale Zahl, η_1 eine Funktion, deren Nenner nicht durch π teilbar ist. Der Funktion ϱ erteile man den Wert 0 und der Funktion η den Wert

$$\eta_0 = \infty, \text{ wenn } m < 0,$$
$$\eta_0 = a, \text{ wenn } m = 0,$$
$$\eta_0 = 0, \text{ wenn } m > 0.$$

4. Die so bestimmten Werte aller Funktionen η genügen den Bedingungen 1. bis 5. und konstituieren also einen Punkt, der durch das Primfunktional π erzeugt heißt.

Man kann also aus einer einzigen Funktion z und den Primfaktoren der Linearformen $z - c$ alle Punkte ableiten, in denen

z einen endlichen Wert hat. Um auch die übrigen zu bestimmen, muß man noch eine zweite Funktion, etwa $z_1 = 1 : z$, zu Hilfe nehmen, die in den noch fehlenden, in endlicher Anzahl vorhandenen Punkten den endlichen Wert 0 hat.

Die Gesamtheit der Punkte bilden die absolute Riemannsche Fläche[1]).

§ 188. Ordnungszahlen.

1. Ist $\mathfrak{P}$ ein Punkt, so schreiben wir jeder Funktion η, die in diesem Punkte einen endlichen und von Null verschiedenen Wert erhält, in $\mathfrak{P}$ die Ordnung 0 zu.

2. Wenn ω die Gesamtheit der in $\mathfrak{P}$ verschwindenden Funktionen durchläuft, und ϱ eine von diesen Funktionen ist, für die alle

$$\frac{\omega}{\varrho}$$

endliche Werte haben, so hat ϱ die Ordnung 1.

Man sagt auch, ϱ wird in $\mathfrak{P}$ unendlich klein in der ersten Ordnung.

Ist $\frac{\varrho'}{\varrho}$ weder Null noch Unendlich, so hat ϱ' hiernach gleichfalls die Ordnung 1. Umgekehrt ist, wenn ϱ und ϱ' beide die Ordnungszahl 1 haben, $\varrho : \varrho'$ und $\varrho' : \varrho$ weder Null noch Unendlich.

3. Ist ϱ von der ersten Ordnung und ω irgend eine Funktion in Ω, so hat ω die Ordnungszahl n, wenn $\varrho^{-n}\omega$ in $\mathfrak{P}$ weder Null noch unendlich wird.

Diese Bestimmung der Ordnung n ist unabhängig davon, welche Funktion erster Ordnung wir genommen haben. Ist n positiv, so wird ω Null, ist n negativ, so wird ω unendlich, und ist $n = 0$, so hat ω in $\mathfrak{P}$ einen endlichen, von Null verschiedenen Wert.

---

[1]) Nach Riemanns Theorie der algebraischen Funktionen entspricht jeder Punkt der geschlossenen mehrblätterigen Fläche einem Punkte in unserem Sinne. Ist z unabhängige Variable, so ist die Riemannsche Fläche n-blätterig über die z-Ebene ausgebreitet. Als absolute Riemannsche Fläche kann man irgend eine Fläche betrachten, auf die die Gesamtheit jener mehrblätterigen Flächen eindeutig und stetig bezogen werden kann.

Die Definition der Ordnungszahl haftet also am Punkte $\mathfrak{P}$. Sie ist für den Körper Ω invariant.

Daß jede Funktion in jedem Punkte $\mathfrak{P}$ eine bestimmte ganze Zahl n als Ordnungszahl erhält, ergibt sich nun aus § 185, (5).

Man nehme eine Funktion z, die in $\mathfrak{P}$ endlich bleibt, als unabhängige Variable, bestimme das zu $\mathfrak{P}$ gehörige Primfunktional π und wähle eine Funktion ϱ, deren Zähler durch π, aber nicht durch π^2 teilbar ist. Diese Funktion ist von der ersten Ordnung.

Dann kann man jede Funktion ω in die Form setzen:

$$(1) \qquad \omega = a\varrho^n + \eta_1 \varrho^{n+1},$$

worin a eine von Null verschiedene Konstante ist, und n ist die Ordnungszahl von ω.

Hat ϱ die Ordnung 1, so hat ϱ^n die Ordnung n.

Über die Ordnungszahlen gelten folgende Sätze, die alle leicht aus (1) folgen:

4. Die Ordnung eines Produktes zweier Funktionen ist gleich der Summe der Ordnungen der Faktoren. Die Ordnung eines Quotienten ist gleich der Differenz der Ordnungen von Zähler und Nenner.

Die Ordnung einer Summe ist gleich der niedrigsten unter den Ordnungen der Summanden. Kommen unter den Summanden mehrere von gleicher niedrigster Ordnungszahl vor, so kann die Ordnung der Summe größer, aber nicht kleiner sein.

Von einer Funktion, die in $\mathfrak{P}$ Null in der $n$ten Ordnung wird, sagt man auch, sie wird Null in der ersten Ordnung in n zusammengefallenen Punkten.

§ 189. Polygone.

1. Definition. Komplexe von Punkten, die denselben Punkt auch mehrmals enthalten können, heißen Polygone oder Vielecke (des Körpers Ω).

Die Zahl der Punkte eines Polygons heißt seine Ordnung, und ein Polygon $m$ter Ordnung wird auch kurz ein m-Eck genannt.

Als Bezeichnung für die Polygone sollen die Buchstaben des großen deutschen Alphabets $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$, ... dienen.

2. Unter dem Produkt $\mathfrak{A}\mathfrak{B}$ zweier Polygone versteht man das Polygon, das die Punkte von $\mathfrak{A}$ und $\mathfrak{B}$ zugleich enthält, und zwar einen Punkt $\mathfrak{P}$, der r mal in $\mathfrak{A}$ und s mal in $\mathfrak{B}$ vorkommt, $r + s$ mal. Die Ordnung eines Produktes ist gleich der Summe der Ordnungen der Faktoren.

Wenn wir also mit $\mathfrak{P}_1, \mathfrak{P}_2, \ldots$ verschiedene Punkte bezeichnen, so können wir jedes Polygon $\mathfrak{A}$ auf eine Weise in die Form setzen:

$$\mathfrak{A} = \mathfrak{P}_1^{r_1}\mathfrak{P}_2^{r_2}\ldots \tag{1}$$

Die Punkte sind also in der Rechnung mit Polygonen die Primelemente. Um auch für die Einheit einen Vertreter zu haben, muß noch das „Nulleck" $\mathfrak{O}$, das gar keinen Punkt enthält, mitgenannt werden.

Der größte gemeinschaftliche Teiler zweier Polygone $\mathfrak{A}$, $\mathfrak{B}$ enthält jeden Punkt, der in $\mathfrak{A}$ und $\mathfrak{B}$ vorkommt, und zwar so oft, als er in jedem von beiden vorkommt.

Das kleinste gemeinschaftliche Vielfache enthält jeden Punkt von $\mathfrak{A}$ und $\mathfrak{B}$, und zwar in der höchsten der Ordnungen, in denen er in $\mathfrak{A}$ und $\mathfrak{B}$ vorkommt.

3. Ist z eine Variable des Körpers Ω und n der Grad des Körpers in bezug auf z, so nimmt z jeden Wert c in n Punkten an.

Denn zerlegt man $z - c$ in seine Primfaktoren [§ 183, (17)]:

$$z - c = \pi_1^{e_1}\pi_2^{e_2}\cdots, \qquad e_1 + e_2 + \cdots = n,$$

so erzeugt jeder dieser Primfaktoren einen Punkt, z. B. π_1 den Punkt $\mathfrak{P}_1$, in dem die Funktion $z - c$ Null in der $e_1$ten Ordnung wird. Rechnet man diesen Punkt e_1 fach, so erhält man ein Polygon $\mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\ldots$ von der Ordnung n, in dessen Punkten die Funktion $z - c$ verschwindet.

Derselbe Satz gilt aber auch für den Wert $c = \infty$, wie man daraus schließt, daß der Grad des Körpers Ω in bezug auf $1 : z$ derselbe ist wie in bezug auf z.

4. Die n Punkte, in denen z einen Wert c annimmt, heißen konjugiert nach z, und die Werte $\eta_1, \eta_2, \ldots, \eta_n$, die eine Funktion η in Ω in n konjugierten Punkten annimmt, heißen gleichfalls konjugiert nach z, und z heißt von der Ordnung n. Die Konstanten, und nur diese, haben die Ordnung 0.

§ 190. Verzweigungspunkte und Verzweigungszahlen.

Nach § 184 gibt es nur eine endliche Anzahl von Punkten, in denen $z - c$ Null in höherer als der ersten Ordnung wird. Diese heißen die Verzweigungspunkte von Ω in z.

Wir konstruieren ein Polygon $\mathfrak{Z}_z$, das $(e-1)$ mal jeden Punkt $\mathfrak{P}$ enthält, in dem $z - c$ oder $1 : z$ Null in der $e$ten Ordnung wird. Dieses Polygon heißt das Verzweigungspolygon von Ω in bezug auf z, und seine Ordnung

$$w_z = \Sigma(e-1) \tag{2}$$

heißt die Verzweigungszahl in bezug auf z[1]).

In § 184, (20) haben wir die Formel erhalten:

$$N(t-\tau) \equiv (t-\tau_1)(t-\tau_2)\dots(t-\tau_n) \pmod{z-c}, \tag{3}$$

worin τ die Basisform des Körpers Ω nach z bedeutet und $\tau_1, \tau_2, \dots, \tau_n$ die gleichen oder verschiedenen konstanten Funktionale, denen τ nach den Primfaktoren von $z - c$ kongruent wird, also die Werte, die τ in den nach z konjugierten Punkten $\mathfrak{P}_1, \mathfrak{P}_2, \dots, \mathfrak{P}_n$ annimmt. In jedem dieser Punkte muß (3) in eine richtige Gleichung übergehen, und daraus folgen z. B.:

$$N(\tau) = \tau_1 \tau_2 \dots \tau_n\,, \tag{4}$$

$$S(\tau) = \tau_1 + \tau_2 + \dots + \tau_n \tag{5}$$

als Werte der rationalen Funktionale $N(\tau)$ und $S(\tau)$ für $z = c$. Setzt man für die Funktionalvariablen rationale Funktionen von z, so gelten entsprechende Formeln für die Funktionen in Ω, vorausgesetzt, daß nicht einer der Ausnahmefälle $0 \cdot \infty$, $\infty + \infty$ eintritt.

Ist daher $\eta_1, \eta_2, \dots, \eta_n$ eine Basis von Ω, und sind $\eta_{i,1}, \eta_{i,2}, \dots, \eta_{i,n}$ konjugierte Werte nach z von η_i, so ist nach (5) und der Definition der Diskriminante in § 173

$$\Delta(\eta_1, \eta_2, \dots, \eta_n) = (\Sigma \pm \eta_{1,1}\, \eta_{2,2} \dots \eta_{n,n})^2. \tag{6}$$

Stehen zwei Funktionen z und z' in Ω in einer linearen Beziehung:

$$z' = \frac{az+b}{cz+\partial}, \tag{7}$$

---

[1]) Breitet man die Riemannsche Fläche über der z-Ebene aus, so ist n die Anzahl der übereinanderliegenden Blätter, w_z ist die Anzahl der Verzweigungspunkte dieser Fläche.

worin a, b, c, ∂ Konstanten sind, deren Determinante $a\partial - bc$ von Null verschieden ist, so sind die Verzweigungspolygone $\mathfrak{Z}_z$ und $\mathfrak{Z}_{z'}$ identisch, und daher ist auch $w_z = w_{z'}$, denn wenn in einem Punkte $z - z_0$ oder $1 : z$ Null in der $e$ten Ordnung wird, so ist in demselben Punkte auch

$$z' - z'_0 = \frac{(a\partial - bc)(z - z_0)}{(cz + \partial)(cz_0 + \partial)}$$

oder wenn z_0 unendlich, also $z'_0 = a : c$ ist:

$$z' - z'_0 = \frac{-(a\partial - bc)}{c(cz + \partial)},$$

und wenn $z'_0 = \infty$, also $cz_0 + \partial = 0$ ist:

$$\frac{1}{z'} = \frac{cz + \partial}{az + b}$$

ebenfalls unendlich klein in der $e$ten Ordnung.

Wenden wir dies auf $z' = 1 : z$ an, so erhalten wir die Verzweigungspunkte, in denen z einen endlichen Wert hat, aus der Körperdiskriminante D_z nach § 184, (24), (28). Es fehlen dann noch die Verzweigungspunkte, in denen $z = \infty$, also $z' = 0$ wird, und diese ergeben sich in gleicher Weise aus den verschwindenden Wurzeln der Körperdiskriminante $D_{z'}$. Demnach haben wir den Satz:

5. Die Verzweigungszahl w_z ist gleich dem Grade der Körperdiskriminante D_z, vermehrt um die Anzahl der verschwindenden Wurzeln von $D_{z'}$. ($z' = 1 : z$).

§ 191. Polygonquotienten und Polygonklassen.

Eine Funktion η in Ω hat nur in einer endlichen Zahl von Punkten eine von Null verschiedene Ordnungszahl. Die Summe der positiven Ordnungszahlen ist ebenso groß wie die Summe der negativen, nämlich gleich der Ordnung der Funktion η (§ 189, 4.). Sind die Ordnungszahlen von η für jeden Punkt $\mathfrak{P}$ bekannt, so ist dadurch die Funktion η bis auf einen konstanten Faktor bestimmt. Denn wenn eine zweite Funktion η' überall dieselben Ordnungszahlen hat, so hat $\eta : \eta'$ überall die Ordnungszahl 0 und ist daher konstant (§ 189, 4.).

Wir bilden ein Polygon $\mathfrak{A}$, in das wir jeden Punkt, in dem η eine positive Ordnungszahl hat, so oft aufnehmen, als diese Ordnungszahl angibt, und ein zweites Polygon $\mathfrak{B}$, in das wir in

entsprechender Weise die Punkte aufnehmen, in denen η eine negative Ordnungszahl hat. Dann sind die Polygone $\mathfrak{A}$ und $\mathfrak{B}$ von gleicher Ordnung, nämlich von der Ordnung der Funktion η, und durch diese Polygone ist die Funktion η bis auf einen konstanten Faktor bestimmt.

Wir können daher die symbolische Bezeichnung einführen:

(1) $$\eta = \frac{\mathfrak{A}}{\mathfrak{B}},$$

und $\mathfrak{A}$ den Zähler oder das Obereck, $\mathfrak{B}$ den Nenner oder das Untereck von η nennen. Nach dieser Definition sind zunächst $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim zueinander. Wir wollen aber diese Bezeichnung noch dadurch erweitern, daß wir, wenn $\mathfrak{M}$ ein beliebiges Polygon ist:

(2) $$\frac{\mathfrak{M}\mathfrak{A}}{\mathfrak{M}\mathfrak{B}} = \frac{\mathfrak{A}}{\mathfrak{B}}$$

setzen. Dann ist die Bezeichnung (1) von der Beschränkung frei, daß $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim sein sollen. Beide Polygone sind immer noch von gleicher Ordnung, aber diese kann größer sein als die Ordnung von η.

Bei dieser Darstellung der Funktionen η gelten dann für die Multiplikation und Division dieselben Regeln, wie beim Rechnen mit Zahlenbrüchen im Gebiete der natürlichen Zahlen.

In (1) können $\mathfrak{A}$, $\mathfrak{B}$ nicht beliebige m-Ecke sein, und die Erforschung der Beziehung zwischen diesen ist die große Frage, die, in anderer Weise, durch das Abelsche Theorem beantwortet wird.

Wir stellen folgende Definition auf:

1. Können zwei n-Ecke $\mathfrak{A}$, $\mathfrak{A}'$ Obereck und Untereck einer Funktion η in Ω sein, so heißen $\mathfrak{A}$ und $\mathfrak{A}'$ äquivalent.

In Zeichen: Gibt es eine Funktion η, der die Bezeichnung

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}$$

zukommt, so ist

(3) $$\mathfrak{A} \sim \mathfrak{A}'.$$

Aus der Formel

$$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}, \quad \eta' = \frac{\mathfrak{A}}{\mathfrak{A}''}, \quad \frac{\eta'}{\eta} = \frac{\mathfrak{A}'}{\mathfrak{A}''}$$

ergibt sich der Satz:

2. Sind zwei n-Ecke mit einem dritten äquivalent, so sind sie auch untereinander äquivalent. Man vereinigt danach äquivalente Polygone $\mathfrak{A}, \mathfrak{A}', \ldots$ in einer Polygonklasse A. Jedes Polygon ist in einer, und nur in einer Klasse enthalten.

Es existieren auch Polygone, die mit keinem anderen äquivalent sind, und die daher jedes für sich eine besondere Klasse bilden. Diese heißen isolierte Polygone.

3. Ist $\mathfrak{A} \sim \mathfrak{A}'$, $\mathfrak{B} \sim \mathfrak{B}'$, so ist $\mathfrak{A}\mathfrak{B} \sim \mathfrak{A}'\mathfrak{B}'$.

Dies folgt aus

(4) $$\eta = \frac{\mathfrak{A}}{\mathfrak{A}'}, \quad \eta_1 = \frac{\mathfrak{B}}{\mathfrak{B}'}, \quad \eta\eta_1 = \frac{\mathfrak{A}\mathfrak{B}}{\mathfrak{A}'\mathfrak{B}'}.$$

Die Klasse C, der das Produkt $\mathfrak{A}\mathfrak{B}$ aus den Klassen A, B angehört, enthält daher alle Produkte aus einem Polygon der Klasse A mit einem Polygon der Klasse B (unter Umständen auch noch andere) und ist daher durch die Klassen A und B vollständig bestimmt. Darauf beruht die Multiplikation (Komposition) der Klassen, die sich in der Formel ausdrückt:

(5) $$C = AB = BA.$$

Aus einer Gleichung zwischen drei Klassen A, B, M

$$MA = MB$$

folgt hiernach $A = B$. Denn ist $\mathfrak{M}\mathfrak{A} \sim \mathfrak{M}\mathfrak{B}$, so folgt aus (2) $\mathfrak{A} \sim \mathfrak{B}$. Ist $\mathfrak{A} \sim \mathfrak{A}'$ und

$$\mathfrak{A}\mathfrak{B} = \mathfrak{C} \quad \text{und} \quad \mathfrak{A}'\mathfrak{B} = \mathfrak{C}',$$

so ist auch $\mathfrak{C} \sim \mathfrak{C}'$. Wenn also $\mathfrak{A}$ in $\mathfrak{C}$ enthalten ist, so ist jedes mit $\mathfrak{A}$ äquivalente Polygon in einem mit $\mathfrak{C}$ äquivalenten Polygon $\mathfrak{C}'$ enthalten.

4. Wir nennen eine Klasse C durch eine Klasse A teilbar, wenn ein Polygon von A in einem Polygon von C enthalten ist, und setzen

(6) $$AB = C.$$

Die Klasse B ist durch A und C vollständig bestimmt.

§ 192. Polygonscharen.

Wenn $\mathfrak{A}, \mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$ Polygone einer Klasse A sind, so gibt es s Funktionen in Ω:

(1) $$\eta_1 = \frac{\mathfrak{A}_1}{\mathfrak{A}}, \quad \eta_2 = \frac{\mathfrak{A}_2}{\mathfrak{A}}, \ldots, \eta_s = \frac{\mathfrak{A}_s}{\mathfrak{A}}.$$

Ist $\mathfrak{P}$ irgend ein Punkt und ϱ eine Funktion, die in diesem Punkt die Ordnung 1 hat, so setzen wir nach § 185

$$
(2) \qquad \begin{aligned}
\eta_1 &= e_1 \varrho^m + \sigma_1 \varrho^{m+1}, \\
\eta_2 &= e_2 \varrho^m + \sigma_2 \varrho^{m+1}, \\
&\cdots\cdots\cdots \\
\eta_s &= e_s \varrho^m + \sigma_s \varrho^{m+1},
\end{aligned}
$$

worin $e_1, e_2, \ldots, e_s$ Konstanten sind, die nicht alle verschwinden, und $\sigma_1, \sigma_2, \ldots, \sigma_s$ Funktionen, die in $\mathfrak{P}$ endlich sind; m ist die niedrigste Ordnungszahl in $\mathfrak{P}$, die unter den Funktionen η_i vorkommt.

Der Inbegriff der Funktionen

$$
(3) \qquad \eta = c_1 \eta_1 + c_2 \eta_2 + \cdots + c_s \eta_s
$$

mit Konstanten $c_1, c_2, \ldots, c_s$ heißt eine Schar. Wir bezeichnen sie durch

$$
(4) \qquad (\eta_1, \eta_2, \ldots, \eta_s),
$$

und nennen $\eta_1, \eta_2, \ldots, \eta_s$ eine Basis der Schar. Die Ordnung von η in $\mathfrak{P}$ ist nicht kleiner als m (sie ist größer, wenn $e_1 c_1 + e_2 c_2 + \cdots + e_s c_s = 0$ ist). Es kann aber η in keinem Punkt $\mathfrak{P}$ unendlich werden, der nicht in $\mathfrak{A}$ enthalten ist, und auch nicht in höhere Ordnung, als der Punkt $\mathfrak{P}$ in $\mathfrak{A}$ eingeht.

Wir können also setzen:

$$
(5) \qquad \eta = \frac{\mathfrak{A}'}{\mathfrak{A}},
$$

worin $\mathfrak{A}'$ gleichfalls zur Klasse A gehört.

Nimmt man statt $\mathfrak{A}$ ein anderes Polygon $\mathfrak{B}$ der Klasse A und setzt

$$
(6) \qquad \zeta = \frac{\mathfrak{A}}{\mathfrak{B}},
$$

so folgt aus 1.:

$$
(7) \qquad \begin{aligned}
\zeta \eta_1 &= \eta_1' = \frac{\mathfrak{A}_1}{\mathfrak{B}}, \\
\zeta \eta_2 &= \eta_2' = \frac{\mathfrak{A}_2}{\mathfrak{B}}, \\
&\cdots\cdots\cdots \\
\zeta \eta_s &= \eta_s' = \frac{\mathfrak{A}_s}{\mathfrak{B}}
\end{aligned}
$$

und

$$
(8) \qquad \zeta \eta = \eta' = c_1 \eta_1' + c_2 \eta_2' + \cdots + c_s \eta_s' = \frac{\mathfrak{A}'}{\mathfrak{B}}.
$$

Jedes durch den Nenner $\mathfrak{A}$ und ein Konstantensystem $c_1, c_2, \ldots, c_s$ erzeugte Polygon $\mathfrak{A}'$ wird also auch durch jeden mit

$\mathfrak{A}$ äquivalenten Nenner und dasselbe Konstantensystem erzeugt, und dies Polygon $\mathfrak{A}'$ ist also nur abhängig von den Konstanten und von den Polygonen $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$. Der Inbegriff dieser Polygone wird eine Polygonschar mit der Basis $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$ genannt und mit

$$(9) \qquad (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s)$$

bezeichnet.

Wenn die Polygone $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$ den größten gemeinschaftlichen Teiler $\mathfrak{M}$ haben, so ist dieser Teiler in allen Polygonen der Schar enthalten und heißt der Teiler der Schar. Aber man kann in der Schar ein Polygon $\mathfrak{A}' = \mathfrak{M}\mathfrak{B}$ so bestimmen, daß $\mathfrak{B}$ beliebig gegebene Punkte nicht enthält.

Denn ist ein Punkt $\mathfrak{P}$ μmal in $\mathfrak{M}$ und νmal in $\mathfrak{A}$ enthalten und ϱ eine Funktion, die in $\mathfrak{P}$ von der ersten Ordnung verschwindet, so ist in den Entwickelungen (2):

$$m = \mu - \nu,$$

und die Entwickelung von $\eta = \mathfrak{A}' : \mathfrak{A} = \mathfrak{M}\mathfrak{B} : \mathfrak{A}$ lautet

$$\eta = e\,\varrho^m + \sigma\,\varrho^{m+1},$$

worin

$$e = e_1 c_1 + e_2 c_2 + \cdots + e_s c_s.$$

Wählt man also die c_i so, daß e nicht verschwindet, so ist $\mathfrak{P}$ nicht in $\mathfrak{B}$ enthalten.

Eine Schar, die einen Teiler $\mathfrak{M}$ hat, heißt eine uneigentliche Schar.

Wenn zwischen den Funktionen $\eta_1, \eta_2, \ldots, \eta_s$ eine Relation von der Form besteht:

$$(10) \qquad c_1\eta_1 + c_2\eta_2 + \cdots + c_s\eta_s = 0,$$

in der die Konstanten $c_1, c_2, \ldots, c_s$ nicht alle $= 0$ sind, so besteht dieselbe Relation

$$(11) \qquad c_1\eta_1' + c_2\eta_1' + \cdots + c_s\eta_s' = 0$$

zwischen den Funktionen (7). Wir nennen dann diese Funktionen linear abhängig. Dem entsprechend heißen auch die Polygone der Schar $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$ linear abhängig. Man kann dann eine der Funktionen, etwa η_s, linear durch die übrigen ausdrücken, und die Schar $(\eta_1, \eta_2, \ldots, \eta_s)$ ist mit $(\eta_1, \eta_2, \ldots, \eta_{s-1})$ identisch. Gleiches gilt von den Polygonscharen $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s)$ und $(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_{s-1})$. Durch wiederholte Anwendung dieser Reduktion kann man jede Schar durch eine linear unabhängige oder irreduzible Basis darstellen. Zwei irreduzible Basen einer

Schar haben gleich viel Elemente, und diese Zahl heißt die Dimension der Schar und die Schar heißt eine s-fache. Sind $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s$ linear abhängig oder unabhängig, so gilt dasselbe von $\mathfrak{M}\mathfrak{A}_1, \mathfrak{M}\mathfrak{A}_2, \ldots, \mathfrak{M}\mathfrak{A}_s$.

Man kann in einer Schar der Dimension $s > 1$

(12) $$S = (\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s)$$

ein Polygon finden, das einen beliebigen Punkt $\mathfrak{P}$ mindestens einmal öfter enthält als der Teiler $\mathfrak{M}$ dieser Schar.

Dieser Zweck wird erreicht, wenn man für diesen Punkt die Entwickelung (2) ansetzt und dann eine der Konstanten $c_1, c_2, \ldots, c_s$ aus der Gleichung

(13) $$c_1 e_1 + c_2 e_2 + \cdots + c_s e_s = 0$$

bestimmt. Diese Polygone bilden dann eine Schar von der $(s-1)$ten Dimension, deren Teiler durch $\mathfrak{M}\mathfrak{P}$ teilbar ist.

Dieser Satz läßt sich dahin erweitern:

5. Die Polygone einer s-fachen Schar, die durch ein r-Eck $\mathfrak{R}$ teilbar sind, bilden eine mindestens $(s-r)$-fache Schar.

Ist dieser Satz schon für ein r-Eck bewiesen, so folgt er für ein $(r+1)$-Eck $\mathfrak{R}\mathfrak{P}$ aus dem vorhergehenden. Denn durch Hinzutreten des Punktes $\mathfrak{P}$ wird entweder die Dimension nicht verändert, wenn $\mathfrak{P}$ im Teiler der durch $\mathfrak{R}$ reduzierten Schar aufgeht, oder sie wird um 1 vermindert.

Man kann das Polygon $\mathfrak{R}$ so wählen, daß die Dimension von S genau auf $(s-r)$ reduziert wird. Zu diesem Zweck hat man die Punkte von $\mathfrak{R}$ successive so zu wählen, daß jeder folgende im Teiler der durch die vorangehende reduzierten Schar nicht enthalten ist. Daraus folgt:

6. In einer s-fachen Schar gibt es mindestens ein Polygon, das durch ein gegebenes $(s-1)$-Eck teilbar ist.

Ist die Klasse A, der alle Polygone der Schar S angehören, von der $m$ten Ordnung, so kann die Dimension s der Schar nicht größer sein als $m+1$. Denn sonst könnte man nach 6. in S ein Polygon finden, das durch ein $(m+1)$-Eck teilbar wäre, was widersinnig ist, da S nur m-Ecke enthält. Es hat daher die Dimension s der Schar bei gegebener Klasse A ein Maximum. Ist dieses Maximum erreicht, so sind alle Polygone der Klasse A

in S enthalten. Denn gibt es ein nicht in S enthaltenes Polygon $\mathfrak{A}_{s+1}$ in A, so ist

$$(\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_s, \mathfrak{A}_{s+1})$$

eine Schar von der Dimension $s + 1$. Damit ist bewiesen:

7. Die Polygone einer Klasse bilden eine Schar von einer endlichen Dimension s. Diese Zahl soll die Dimension der Klasse heißen.

Wenn es in einer Klasse C Polygone gibt, die durch ein Polygon $\mathfrak{A}$ einer Klasse A teilbar sind, so ist C durch A teilbar. Ist

$$C = AB,$$

so erhält man die Dimension von B dadurch, daß man die Schar aus C aussucht, die durch irgend ein Polygon $\mathfrak{A}$ in A teilbar ist. Diese Dimension ist also nur von den beiden Klassen A und C abhängig und soll mit (A, C) bezeichnet werden. Das Zeichen für die Dimension einer Klasse A ist hiernach (O, A), wenn O die Klasse des Nullecks ist. Wir haben dann

(14) $$(A, C) = (A, AB) = (O, B),$$

und wenn a die Ordnung der Klasse A ist, so ist nach 5.:

(15) $$(A, C) \gtreqless (O, C) - a.$$

Bezeichnen wir mit A die eigentliche Klasse, die man erhält, wenn man $\mathfrak{M}$ überall weghebt, so soll die uneigentliche Klasse mit dem Teiler $\mathfrak{M}$ durch $\mathfrak{M}A$ bezeichnet sein.

8. Der Teiler einer uneigentlichen Klasse ist ein isoliertes Polygon.

Ist nämlich $\mathfrak{M}A$ eine uneigentliche Klasse, so läßt sich in A ein Polygon $\mathfrak{A}$ finden, das relativ prim zu $\mathfrak{M}$ ist. Ist $\mathfrak{M}'$ mit $\mathfrak{M}$ äquivalent, so ist $\mathfrak{M}'\mathfrak{A}$ in $\mathfrak{M}A$ enthalten und mithin durch $\mathfrak{M}$ teilbar. Es ist also auch $\mathfrak{M}'$ durch $\mathfrak{M}$ teilbar, also mit $\mathfrak{M}$ identisch. Es gibt also in der Klasse von $\mathfrak{M}$ nur das einzige Polygon $\mathfrak{M}$.

§ 193. Normalbasen.

Nach dem Vorigen können wir eine Funktion z des Körpers Ω von der $n$ten Ordnung in der Form

(1) $$z = \frac{\mathfrak{U}'}{\mathfrak{U}}$$

darstellen, worin $\mathfrak{U}$ und $\mathfrak{U}'$ äquivalente n-Ecke ohne gemeinschaftlichen Teiler sind. Eine ganze Funktion ω von z ist dadurch charakterisiert, daß sie in keinem Punkt unendlich wird, der nicht in $\mathfrak{U}$ enthalten ist. Folglich läßt sich eine solche Funktion ω so darstellen:

(2) $$\omega = \frac{\mathfrak{A}}{\mathfrak{U}^r},$$

worin r ein positiver Exponent ist. In (2) können Zähler und Nenner gemeinschaftliche Teiler haben. Wir können aber annehmen, daß $\mathfrak{A}$ nicht durch $\mathfrak{U}$ teilbar ist. Dann hat in (2) der Exponent r den kleinst möglichen Wert. Diese Zahl r soll der Exponent von ω in z heißen.

1. Setzen wir $z' = 1 : z$, so ist nach (1), (2):

$$z' = \frac{\mathfrak{U}}{\mathfrak{U}'}, \quad \omega' = \omega z'^r = \frac{\mathfrak{A}}{\mathfrak{U}'^r},$$

und wenn $\mathfrak{A}$ nicht durch $\mathfrak{U}'$ teilbar ist, so ist r der Exponent von ω' in bezug auf z'. Die Annahme, daß $\mathfrak{A}$ nicht durch $\mathfrak{U}'$ teilbar sei, bedeutet, daß ω nicht durch z teilbar sei, und daraus folgt, daß auch ω' nicht durch z' teilbar ist.

2. Der Exponent einer ganzen rationalen Funktion von z vom $m$ten Grade

$$x = a_0 + a_1 z + \cdots + a_m z^m$$

ist gleich m. Denn diese Funktion wird in jedem in $\mathfrak{U}$ enthaltenen Punkt unendlich von der $m$ten Ordnung. Der Exponent des Produktes $x\omega$ ist gleich $r + m$.

3. Der Exponent einer Summe

$$\omega = c_1 \omega_1 + c_2 \omega_2 + \cdots + c_s \omega_s$$

ist höchstens gleich dem größten der Exponenten von $\omega_1, \omega_2, \ldots, \omega_s$.

4. Wir bestimmen eine Reihe ganzer Funktionen von z

$$\lambda_1, \lambda_2, \lambda_3, \ldots$$

durch folgende recurrente Bestimmung:

1) λ_1 konstant (Exponent $r_1 = 0$),

2) λ_2 eine nicht rationale ganze Funktion von z mit möglichst kleinem Exponenten r_2,

3) λ_s eine nicht in der Form

(3) $$x_1 \lambda_1 + x_2 \lambda_2 + \cdots + x_{s-1} \lambda_{s-1}$$

enthaltene ganze Funktion von z mit möglichst kleinem Exponenten r_s,

und setzen diese Reihe fort, solange man noch Funktionen λ_s finden kann, die nicht in der Form (3) enthalten sind.

Nach 4., 3) sind die Funktionen $\lambda_1, \lambda_2, \ldots, \lambda_s$ in dem Sinne linear unabhängig, daß zwischen ihnen keine lineare Gleichung besteht mit rationalen Koeffizienten in z. Da es nicht mehr als n linear unabhängige Funktionen gibt, so kann s nicht größer als n sein. Andererseits gibt es, solange $s \overline{\gtrless} n$ ist, immer noch ganze Funktionen, die von $\lambda_1, \lambda_2, \ldots, \lambda_{s-1}$ nicht linear abhängig sind, und darunter auch solche von kleinstem Exponenten. Wir erhalten also n Funktionen

(4) $$L = (\lambda_1, \lambda_2, \ldots, \lambda_n),$$

und diese bilden eine Basis des Körpers Ω nach z. Sie bilden eine Minimalbasis; denn wäre dies nicht der Fall, so müßte für irgend ein $s \overline{\gtrless} n$ eine Funktion $x_1 \lambda_1 + x_2 \lambda_2 + \cdots + x_s \lambda_s$ durch eine lineare Funktion $z - c$ teilbar sein, ohne daß x_s durch $z - c$ teilbar ist. Reduziert man $x_1, x_2, \ldots, x_s$ auf ihre Reste nach $z - c$, so ergibt sich eine Gleichung:

$$c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_s \lambda_s = (z - c) \mu,$$

worin die $c_1, c_2, \ldots, c_s$ konstant sind, c_s von Null verschieden und μ eine ganze Funktion ist. Es ist μ nicht in der Form (3) enthalten und sein Exponent ist nach 2. und 3. kleiner als der Exponent von λ_s, was der Bestimmung 4. 3) widerspricht. Also:

5. Die Funktionen $\lambda_1, \lambda_2, \ldots, \lambda_n$ bilden eine Minimalbasis von Ω nach z. Sie heißt eine Normalbasis.

Die Exponenten $r_1, r_2, r_3, \ldots, r_n$ dieser Funktionen genügen der Bedingung:

(5) $$r_1 = 0, \quad 1 \overline{\gtrless} r_2 \overline{\gtrless} r_3 \ldots \overline{\gtrless} r_n.$$

Denn wäre $r_s < r_{s-1}$, so hätte man nach 3. 3) λ_s an Stelle von λ_{s-1} nehmen müssen.

Von den Funktionen λ_i ist keine durch z teilbar; denn wäre $\lambda_s = z\mu$, so hätte μ einen kleineren Exponenten als λ_s und wäre nicht in der Form (3) enthalten. Es müßte also μ an Stelle von λ_s treten.

6. Demnach sind (nach 1.)

$$r_1, r_2, \ldots, r_n$$

die Exponenten von

(6) $$\lambda_1' = z'^{r_1} \lambda_1, \quad \lambda_2' = z'^{r_2} \lambda_2, \ldots, \lambda_n' = z'^{r_n} \lambda_n$$

in bezug auf $z' = 1 : z$, und diese Funktionen sind die Elemente einer Normalbasis von Ω nach z'.

Bezeichnen wir nämlich mit x'_i ganze rationale Funktionen von z', höchstens vom Grade m, so ist

(7) $$x_i = z^m x'_i$$

eine ganze rationale Funktion von z. Wäre nun

$$\lambda'_s = \sum_{0,\, s-1}^{i} x'_i \lambda'_i,$$

so würde aus (6) und (7) folgen:

$$z^m \lambda_s = \sum_{0,\, s-1}^{i} x_i z^{r_s - r_i} \lambda_i,$$

und dies ist unmöglich, weil die λ_i linear unabhängig sind; und es kann auch keine Funktion λ'_s von niedrigerem Exponenten als r_s geben, weil man daraus eine Funktion λ_s von niedrigerem Exponenten herleiten könnte.

Die Körperdiskriminanten D_z, $D_{z'}$ in bezug auf die Variable z und z' sind

$$D_z = \Delta(\lambda_1, \lambda_2, \ldots, \lambda_n),$$
$$D_{z'} = \Delta(\lambda'_1, \lambda'_2, \ldots, \lambda'_n),$$

und daraus folgt nach (6):

(8) $$D_{z'} = z'^{\,2(r_1 + r_2 + \cdots + r_n)} D_z.$$

Ist also δ der Grad von D_z, so ist

$$2(r_1 + r_2 + \cdots + r_n) - \delta$$

die Anzahl der verschwindenden Wurzeln von $D_{z'}$, und es ergibt sich nach § 190, 5.:

(9) $$w_z = 2(r_1 + r_2 + \cdots + r_n).$$

7. **Die Verzweigungszahl w_z ist also immer eine gerade Zahl.**

§ 194. Differentialquotienten.

Die Differentialquotienten können wir, wo wir keinen Gebrauch von der Stetigkeit machen, nicht in der gewöhnlichen Weise einführen. Wir nehmen zwei Funktionen α, β aus Ω, zwischen denen die irreduzible Gleichung

(1) $$F(\alpha, \beta) = 0$$

besteht, bezeichnen mit $F'(\alpha)$, $F'(\beta)$ die abgeleiteten Funktionen und definieren den Differentialquotienten als Funktion des Körpers Ω durch die Formel:

(2) $$\left(\frac{d\alpha}{d\beta}\right) = -\frac{F'(\beta)}{F'(\alpha)}.$$

Es seien α_0, β_0 die endlichen Werte der Funktionen α, β in einem Punkt $\mathfrak{P}$. Dann ist $F(\alpha_0, \beta_0) = 0$, und wir können die Gleichung (1) so darstellen:

$$(3) \quad 0 = (\alpha - \alpha_0) F'(\alpha_0) + (\beta - \beta_0) F'(\beta_0) \\ + \tfrac{1}{2}[(\alpha - \alpha_0)^2 F''(\alpha_0, \alpha_0) + 2(\alpha - \alpha_0)(\beta - \beta_0) F''(\alpha_0, \beta_0) \\ + (\beta - \beta_0)^2 F''(\beta_0, \beta_0)] + \cdots$$

Die beiden zueinander reziproken Funktionen

$$\frac{\alpha - \alpha_0}{\beta - \beta_0}, \quad \frac{\beta - \beta_0}{\alpha - \alpha_0}$$

können nicht beide in dem Punkt $\mathfrak{P}$ unendlich sein. Es sei also:

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0$$

der endliche Wert des ersten dieser Quotienten. Dann ergibt sich aus (3), wenn $F'(\alpha_0)$ nicht Null ist:

$$(4) \quad \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 = -\frac{F'(\beta_0)}{F'(\alpha_0)} = -\left(\frac{F'(\beta)}{F'(\alpha)}\right)_0 = \left(\frac{d\alpha}{d\beta}\right)_0.$$

Diese Gleichung besteht für alle Punkte $\mathfrak{P}$, mit etwaiger Ausnahme einer endlichen Anzahl[1]).

1. Eine Funktion η in Ω, die in allen Punkten, mit Ausnahme einer endlichen Anzahl, der Bedingung genügt:

$$(5) \quad \eta_0 = \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0$$

ist mit $\left(\frac{d\alpha}{d\beta}\right)$ identisch.

Denn aus (4) und (5) folgt, daß die Funktion

$$\left(\frac{d\alpha}{d\beta}\right) - \eta$$

unendlich viele Nullpunkte hat und daher identisch verschwinden muß.

Die Formel (5) kann also gleichfalls als Definition des Differentialquotienten dienen.

Daraus ergeben sich einfach die Hauptsätze über die Differentialquotienten:

---

[1]) Unter den auszunehmenden Punkten sind jedenfalls die enthalten, in denen α_0 oder β_0 unendlich wird. Denn für diese Punkte sind die Funktionen $\alpha - \alpha_0$, $\beta - \beta_0$ gar nicht erklärt.

2. Seien α, β, γ drei Funktionen in Ω; dann ist

$$\left(\frac{d\alpha}{d\beta}\right)\left(\frac{d\beta}{d\gamma}\right) = \left(\frac{d\alpha}{d\gamma}\right). \tag{6}$$

Denn es ist für unendlich viele Punkte

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 \left(\frac{\beta - \beta_0}{\gamma - \gamma_0}\right)_0 = \left(\frac{\alpha - \alpha_0}{\gamma - \gamma_0}\right)_0,$$

und daraus folgt wie bei 1. der Satz 2.

Demnach kann man jeder Funktion α in Ω eine Funktion $d\alpha$ so zuordnen, daß für irgend zwei dieser Funktionen:

$$\left(\frac{d\alpha}{d\beta}\right) = \frac{d\alpha}{d\beta} \tag{7}$$

ein wirklicher Quotient zweier Funktionen $d\alpha$, $d\beta$ wird. Diese Funktionen nennen wir die Differentiale von α, β. Die Differentiale der Konstanten und nur diese sind gleich Null. Die anderen Differentiale sind alle vollständig bestimmt, wenn eines von ihnen willkürlich (z. B. konstant) angenommen ist.

3. Sind α, β, γ, ..., beliebige Funktionen in Ω, die einer Gleichung

$$F(\alpha, \beta, \gamma, \ldots) = 0 \tag{8}$$

genügen, so ist

$$F'(\alpha)\, d\alpha + F'(\beta)\, d\beta + F'(\gamma)\, d\gamma + \cdots = 0. \tag{9}$$

Um diesen Satz zu beweisen, nehme man einen Punkt $\mathfrak{P}$, in dem keine der Funktionen α, β, γ ... oder $d\alpha$, $d\beta$, $d\gamma$, ... unendlich oder Null wird und auch die abgeleiteten $F'(\alpha)$, $F'(\beta)$, $F'(\gamma)$ nicht verschwinden, und ordnen wie in (3) die Funktion F nach Potenzen und Produkten von $\alpha - \alpha_0$, $\beta - \beta_0$, $\gamma - \gamma_0$, ... Dann ergibt sich, daß die Gleichung (9) für unendlich viele Punkte, und mithin identisch erfüllt ist. Als Spezialfälle von (9) ergeben sich:

$$\begin{aligned} d(\alpha + \beta) &= d\alpha + d\beta, \\ d(\alpha\beta) &= \beta\, d\alpha + \alpha\, d\beta, \\ d\left(\frac{\alpha}{\beta}\right) &= \frac{\beta\, d\alpha - \alpha\, d\beta}{\beta^2}. \end{aligned} \tag{10}$$

Der Begriff des Differentials läßt sich ohne weiteres auf holomorphe Funktionale übertragen, wenn die Funktionalvariablen als Konstanten betrachtet werden. Der Satz 3. und die daraus folgenden Formeln (10) gelten dann auch noch, wenn α, β, γ, ... holomorphe Funktionale sind und $F(\alpha, \beta, \gamma, \ldots)$ eine ganze rationale Funktion von α, β, γ, ..., ist.

Ist α eine ganze rationale Funktion von z, so ist $d\alpha/dz$ ebenfalls eine ganze rationale Funktion, nämlich die Derivierte von α nach z.

§ 195. Darstellung der Differentialquotienten durch Polygonquotienten.

Wir nehmen irgend eine Funktion z der $n$ten Ordnung in Ω und eine Minimalbasis $\omega_1, \omega_2, \ldots, \omega_n$ in bezug auf z. Alle ganzen Funktionen von z des Körpers Ω sind dann in der Form darstellbar:

$$\omega = x_1 \omega_1 + x_2 \omega_2 + \cdots + x_n \omega_n \tag{1}$$

und gehen aus dem Basisfunktional

$$\tau = t_1 \omega_1 + t_2 \omega_2 + \cdots + t_n \omega_n \tag{2}$$

hervor, wenn für die Funktionalvariablen $t_1, t_2, \ldots, t_n$ ganze rationale Funktionen $x_1, x_2, \ldots, x_n$ von z gesetzt werden.

Setzen wir, wie in § 184,

$$N(t - \tau) = F(t, z),$$

so genügt τ der irreduzibeln rationalen Gleichung:

$$F(\tau, z) = 0,$$

und man erhält nach § 194, 3.:

$$F'(\tau)\,d\tau + F'(z)\,dz = 0, \tag{3}$$

und hierin ist $F'(\tau)$ das Verzweigungsfunktional (§ 184).

Nach (1) und (2) ist

$$d\omega = d\tau + \omega_1\,dx_1 + \omega_2\,dx_2 + \cdots + \omega_n\,dx_n, \tag{4}$$

wo in $d\tau$ die t_i durch die x_i zu ersetzen sind, und es folgt also aus (3) der Satz:

4. Ist ω eine ganze Funktion von z, so ist

$$F'(\tau)\frac{d\omega}{dz} = -F'(z) + \omega_1 \frac{dx_1}{dz} + \cdots + \omega_n \frac{dx_n}{dz} \tag{5}$$

ein ganzes Funktional.

Andererseits ist $F'(\omega)$ nach § 182, 8. durch $F'(\tau)$ teilbar. Setzen wir also:

$$F'(\omega) = \varrho\, F'(\tau), \tag{6}$$

so ist ϱ ein ganzes Funktional, und aus (4) ergibt sich, wenn man die t_i durch die x_i ersetzt:

$$(7)\qquad -F'(z) = F'(\omega)\left(\frac{d\,\omega}{d\,z} - \omega_1\frac{d\,x_1}{d\,z} - \cdots - \omega_n\frac{d\,x_n}{d\,z}\right)$$
$$= \varrho\,F'(\tau)\left(\frac{d\,\omega}{d\,z} - \omega_1\frac{d\,x_1}{d\,z} - \cdots - \omega_n\frac{d\,x_n}{d\,z}\right),$$

und daraus folgt, daß auch $F'(z)$ (nach Ersetzung der t_i durch die x_i) durch ϱ teilbar ist.

Wir nennen demnach, mit Rücksicht auf die geometrische Analogie, ϱ das Funktional der Doppelpunkte in ω, z.

Ist $\mathfrak{P}$ ein Punkt, in dem z endlich und $F'(\tau)$ von Null verschieden ist, der also kein Verzweigungspunkt in z ist, so hat eine ganze Funktion ω von z nach 4. in $\mathfrak{P}$ einen endlichen Differentialquotienten. Eine gebrochene Funktion η von z, die in $\mathfrak{P}$ endlich ist, läßt sich als Quotient zweier ganzer Funktionen $\omega' : \omega$ darstellen, deren Nenner ω in $\mathfrak{P}$ nicht verschwindet.

Daraus folgt:

$$\frac{d\,\eta}{d\,z} = \frac{1}{\omega^2}\left(\omega'\frac{d\,\omega}{d\,z} - \omega\frac{d\,\omega'}{d\,z}\right),$$

und folglich ist $d\,\eta : d\,z$ im Punkt $\mathfrak{P}$ gleichfalls endlich.

Um das Verhalten eines beliebigen Differentialquotienten $d\,\alpha : d\,\beta$ in irgend einem Punkt $\mathfrak{P}$ zu erkennen, nehme man eine Funktion z, die in $\mathfrak{P}$ Null von der ersten Ordnung wird, und bezeichne mit r, s die Ordnungszahlen von $\alpha - \alpha_0$, $\beta - \beta_0$ in Punkt $\mathfrak{P}$. Für den Fall, daß α in $\mathfrak{P}$ unendlich wird, setze man $\alpha_0 = 0$ und erhält eine negative Ordnungszahl r. Entsprechendes gilt, wenn β unendlich wird.

Dann ist nach § 185:

$$(8)\qquad \begin{aligned} \alpha - \alpha_0 &= z^r\,\alpha', \\ \beta - \beta_0 &= z^s\,\beta', \end{aligned}$$

worin α' und β' Funktionen in Ω sind, die in $\mathfrak{P}$ weder Null noch unendlich werden.

Daraus ergibt sich nach § 194:

$$\frac{d\,\alpha}{d\,z} = r\,z^{r-1}\,\alpha' + z^r\frac{d\,\alpha'}{d\,z},$$
$$\frac{d\,\beta}{d\,z} = s\,z^{s-1}\,\beta' + z^s\frac{d\,\beta'}{d\,z},$$

$$(9)\qquad \frac{\beta - \beta_0}{\alpha - \alpha_0}\,\frac{d\,\alpha}{d\,\beta} = \frac{r + z\dfrac{d\,\alpha'}{\alpha'\,d\,z}}{s + z\dfrac{d\,\beta'}{\beta'\,d\,z}},$$

und wenn man in den Punkt $\mathfrak{P}$ geht:

$$\left(\frac{\beta - \beta_0}{\alpha - \alpha_0} \frac{d\alpha}{d\beta}\right)_0 = \frac{r}{s}, \tag{10}$$

was ein endlicher von Null verschiedener Wert ist.

Daraus folgt:

5. Die Ordnungszahl des Differentialquotienten $d\alpha : d\beta$ in irgend einem Punkt $\mathfrak{P}$ ist gleich der Differenz der Ordnungszahlen von $\alpha - \alpha_0$ und $\beta - \beta_0$.

Ist $r > s$, oder $r < s$, so ist

$$\left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0 = 0 \text{ oder } = \infty,$$

und folglich nach (10) auch

$$\left(\frac{d\alpha}{d\beta}\right)_0 = 0 \text{ oder } = \infty.$$

Ist $r = s$, so folgt aus (10)

$$\left(\frac{d\alpha}{d\beta}\right)_0 = \left(\frac{\alpha - \alpha_0}{\beta - \beta_0}\right)_0. \tag{11}$$

Hier ist jede Spur der Variablen z herausgefallen, und diese Formel gilt für jeden Punkt $\mathfrak{P}$ ohne Ausnahme.

Danach lassen sich die Nullpunkte und Unendlichkeitspunkte der Differentialquotienten genau feststellen und damit diese Funktionen als Polygonquotienten darstellen.

Ist a die Ordnungszahl von $\alpha - \alpha_0$ in einem Punkt $\mathfrak{P}$ nach § 188, so enthält das Verzweigungspolygon $\mathfrak{Z}_\alpha$ den Punkt $\mathfrak{P}$ $a - 1$ mal oder $- a - 1$ mal, je nachdem a positiv oder negativ ist. Ist a negativ, so enthält das Nennerpolygon $\mathfrak{A}$ von α den Punkt $\mathfrak{P}$ $(-a)$ mal, und folglich ist in beiden Fällen der Punkt $\mathfrak{P}$ in $\mathfrak{Z}_\alpha : \mathfrak{A}^2$ $(a - 1)$ mal enthalten. Hat $\mathfrak{Z}_\beta$, $\mathfrak{B}$, b die entsprechende Bedeutung für β, so enthält also der Quotient:

$$\frac{\mathfrak{Z}_\alpha \mathfrak{B}^2}{\mathfrak{Z}_\beta \mathfrak{A}^2}$$

$(a - b)$ mal den Punkt $\mathfrak{P}$.

Die Ordnungszahl von $d\alpha : d\beta$ in $\mathfrak{P}$ ist aber nach 5. ebenso groß, und daraus ergibt sich die Darstellung:

$$\frac{d\alpha}{d\beta} = \frac{\mathfrak{Z}_\alpha \mathfrak{B}^2}{\mathfrak{Z}_\beta \mathfrak{A}^2}, \tag{12}$$

worin, um es zu wiederholen, $\mathfrak{Z}_\alpha$, $\mathfrak{Z}_\beta$ die Verzweigungspolygone, $\mathfrak{A}$, $\mathfrak{B}$ die Nenner von α, β sind.

§ 196. Geschlecht des Körpers Ω.

Da in einem Polygonquotienten Zähler und Nenner von gleicher Ordnung sind, so folgt aus der letzten Formel [§ 195, (12)]:

$$w_\alpha - 2a = w_\beta - 2b. \tag{1}$$

Bezeichnen wir also mit n die Ordnung und mit w die Verzweigungszahl für eine beliebige Variable, die, wie wir im § 193 gesehen haben, eine gerade Zahl ist, so ist die ganze Zahl:

$$p = \tfrac{1}{2}w - n + 1, \tag{2}$$

eine zu dem Körper Ω gehörige invariante ganze Zahl, die das Geschlecht des Körpers genannt wird. Daß diese Zahl nicht negativ sein kann, ergibt sich aus § 193, (5) und (9), wonach

$$p = (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1) \tag{3}$$

ist, und so aus lauter Summanden besteht, deren keiner negativ ist.

Zwei Funktionen α, β nennen wir ein primitives Paar des Körpers Ω, wenn alle Funktionen in Ω rational durch α und β ausgedrückt werden können. Ist α von der $m$ten, β von der $n$ten Ordnung, so ist nach § 171 für ein primitives Paar notwendig und hinreichend, daß die zwischen α und β bestehende irreduzible Gleichung:

$$F(\overset{n}{\alpha}, \overset{m}{\beta}) = 0 \tag{4}$$

in α vom $n$ten, in β vom $m$ten Grade sei.

Es sollen die Funktionen $F'(\alpha)$, $F'(\beta)$ durch Polygonquotienten dargestellt werden. Wir setzen:

$$\alpha = \frac{\mathfrak{M}}{\mathfrak{A}}, \quad \beta = \frac{\mathfrak{N}}{\mathfrak{B}}, \tag{5}$$

worin $\mathfrak{A}$, $\mathfrak{M}$ von der $m$ten, $\mathfrak{B}$, $\mathfrak{N}$ von der $n$ten Ordnung sind. $\mathfrak{A}$ hat dann mit $\mathfrak{M}$ und $\mathfrak{B}$ mit $\mathfrak{N}$ keinen Punkt gemein. Wir setzen:

$$\begin{aligned} F(\alpha, \beta) &= a_0\alpha^n + a_1\alpha^{n-1} + \cdots + a_n, \\ F'(\alpha) &= n a_0\alpha^{n-1} + (n-1)a_1\alpha^{n-2} + \cdots + a_{n-1}, \\ \alpha F'(\alpha) &= -a_1\alpha^{n-1} - 2a_2\alpha^{n-2} - \cdots - n a_n. \end{aligned} \tag{6}$$

Aus der zweiten dieser Gleichungen schließt man, daß im Nenner von $F'(\alpha)$ keine Punkte vorkommen, die nicht in $\mathfrak{A}$ oder in $\mathfrak{B}$ enthalten sind, und aus dem dritten folgt, daß dieser Nenner höchstens $= \mathfrak{A}^{n-2}\mathfrak{B}^m$ sein kann. Wir setzen also:

$$F'(\alpha) = \frac{\mathfrak{Q}}{\mathfrak{A}^{n-2}\mathfrak{B}^m}. \tag{7}$$

Es soll jetzt bewiesen werden, daß $\mathfrak{L}$ durch das Verzweigungspolygon $\mathfrak{Z}_\beta$ teilbar ist.

Nehmen wir zunächst an, daß $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim zu $\mathfrak{Z}_\beta$ seien; dann gibt es eine ganze rationale Funktion x von β, die in keinem Punkt von $\mathfrak{Z}_\beta$ verschwindet, für die $\omega = x\alpha$ eine ganze Funktion von β wird. Setzen wir

$$f(\omega) = x^n F(\alpha, \beta),$$

so ist:

$$f'(\omega) = x^{n-1} F'(\alpha).$$

Ist τ die Basisform von Ω in bezug auf β, so ist nach § 182 $f'(\omega)$ durch $f'(\tau)$ teilbar, und da nach Voraussetzung β in keinem Verzweigungspunkt unendlich wird, so ist $f'(\tau)$ und folglich auch $F'(\alpha)$ durch das Verzweigungspolygon $\mathfrak{Z}_\beta$ teilbar, und unsere Behauptung erwiesen. Wir setzen:

$$\mathfrak{L} = \mathfrak{R}\,\mathfrak{Z}_\beta,$$

(8)
$$F'(\alpha) = \frac{\mathfrak{R}\,\mathfrak{Z}_\beta}{\mathfrak{A}^{n-2}\,\mathfrak{B}^m}.$$

Diese Formel ist hierdurch nur unter der Voraussetzung erwiesen, daß weder α noch β in einem der Verzweigungspunkte unendlich wird.

Machen wir aber die lineare Substitution:

(9)
$$\alpha(\alpha_1 + 1) = a\,\alpha_1, \quad \beta(\beta_1 + 1) = b\,\beta_1,$$

so ist nach § 190

$$\mathfrak{Z}_\beta = \mathfrak{Z}_{\beta_1},$$

und wir können die Konstanten a, b so wählen, daß α_1 und β_1 in keinem Punkte von $\mathfrak{Z}_\beta$ unendlich werden. Wir haben nur für a und b irgend konstante Werte zu nehmen, die α und β in keinem Punkte von $\mathfrak{Z}_\beta$ annehmen.

Ist $F_1(\alpha_1, \beta_1) = 0$ die zwischen α_1, β_1 bestehende rationale Gleichung, so ist:

$$F_1(\alpha_1, \beta_1) = (\alpha_1 + 1)^n (\beta_1 + 1)^m F(\alpha, \beta),$$

oder auch nach (9):

$$\alpha^n \beta^m F_1(\alpha_1, \beta_1) = a^n b^m \alpha_1^n \beta_1^m F(\alpha, \beta);$$

ferner $d\alpha : d\alpha_1 = \alpha^2 : a\,\alpha_1^2$, und folglich, mit Rücksicht auf $F = 0$, $F_1 = 0$:

(10)
$$\alpha^{n-2} \beta^m F_1'(\alpha_1) = a^{n-1} b^m \alpha_1^{n-2} \beta_1^m F'(\alpha).$$

Nach (9) verschwinden α_1, β_1 in denselben Punkten und mit denselben Ordnungszahlen wie α, β, und daraus ergeben sich, den Darstellungen (2) und (4) entsprechend, die Polygondarstellungen:

$$(11) \qquad \alpha_1 = \frac{\mathfrak{M}}{\mathfrak{A}_1}, \quad \beta_1 = \frac{\mathfrak{N}}{\mathfrak{B}_1},$$

und aus (5), (7) und (10):

$$(12) \qquad F_1'(\alpha_1) = \frac{\mathfrak{L}}{\mathfrak{A}_1^{n-2}\,\mathfrak{B}_1^{m}}.$$

Damit ist die Formel (8) allgemein bewiesen.

Setzt man nach § 194, (9):

$$F'(\alpha)\,d\alpha + F'(\beta)\,d\beta = 0,$$

so folgt aus (8) und § 195, (12):

$$(13) \qquad F'(\beta) = \frac{\mathfrak{R}\,\mathfrak{Z}_\alpha}{\mathfrak{A}^n\,\mathfrak{B}^{m-2}}.$$

Beide Ableitungen $F'(\alpha)$, $F'(\beta)$ verschwinden also in den Punkten von $\mathfrak{R}$, und $\mathfrak{R}$ heißt das Polygon der Doppelpunkte in (α, β).

Die Ordnung von $\mathfrak{A}^n\,\mathfrak{B}^{m-2}$ ist $2n(m-1)$ und daraus ergibt sich für die Ordnung $2r$ von $\mathfrak{R}$ eine gerade Zahl, nämlich:

$$2r = 2n(m-1) - w_\alpha = 2m(n-1) - w_\beta,$$

und für das Geschlecht p ergibt sich nach (2):

$$(14) \qquad p = (n-1)(m-1) - r.$$

Siebenundzwanzigster Abschnitt.

Algebraische und Abelsche Differentiale.

§ 197. Differentiale in Ω.

Sind z und z_1 zwei Variable in Ω von den Ordnungen n, n_1 mit den Unterecken $\mathfrak{U}$, $\mathfrak{U}_1$, mit den Verzweigungsecken: $\mathfrak{Z}$, $\mathfrak{Z}_1$, den Verzweigungszahlen w, w_1, so ist nach § 195, (12)

$$\frac{dz}{dz_1} = \frac{\mathfrak{Z}\,\mathfrak{U}_1^2}{\mathfrak{Z}_1\,\mathfrak{U}^2}.$$

Setzt man

$$(1) \qquad \omega = \frac{\mathfrak{A}\,\mathfrak{U}^2}{\mathfrak{B}\,\mathfrak{Z}}, \quad \omega_1 = \frac{\mathfrak{A}\,\mathfrak{U}_1^2}{\mathfrak{B}\,\mathfrak{Z}_1},$$

so wird hiernach

$$(2) \qquad \omega\, dz = \omega_1\, dz_1.$$

Ist $\mathfrak{A}\,\mathfrak{U}^2$ äquivalent mit $\mathfrak{B}\,\mathfrak{Z}$, so ist ω eine Funktion in Ω, und ω_1 ist gleichfalls eine Funktion in Ω. Sind a, b die Ordnungen von $\mathfrak{A}$ und $\mathfrak{B}$, so ist [§ 196, (2)]

$$(3) \qquad \begin{aligned} b + w &= a + 2n, \\ a &= b + 2p - 2, \end{aligned}$$

wenn p das Geschlecht des Körpers Ω ist.

Wir setzen jetzt in einer neuen symbolischen Bezeichnung

$$(4) \qquad dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2},$$

$$(5) \qquad \omega\, dz = dJ = \frac{\mathfrak{A}}{\mathfrak{B}},$$

und nennen diese Ausdrücke die zum Körper Ω gehörigen Differentiale.

Im Zähler und Nenner $\mathfrak{A}$, $\mathfrak{B}$ eines Differentials können gemeinschaftliche Faktoren zugefügt oder weggelassen werden. Haben $\mathfrak{A}$ und $\mathfrak{B}$ keinen gemeinschaftlichen Teiler, so heißt $\mathfrak{A}$ das Obereck, $\mathfrak{B}$ das Untereck des Differentials dJ.

Die Bezeichnung (5) eines Differentials unterscheidet sich von der ähnlichen Bezeichnung der Funktionen in Ω dadurch, daß der Grad des Zählers um $(2p - 2)$ höher ist als der des Nenners.

Die in § 194 definierte Differentiale $d\alpha$ der Funktionen in Ω sind spezielle Fälle der allgemeinen Differentiale (5). Denn nicht alle diese dJ sind Differentiale von Funktionen in Ω. Wir unterscheiden eigentliche Differentiale $d\alpha$, d. h. solche, die Differentiale von Funktionen in Ω sind, und uneigentliche oder Abelsche Differentiale dJ, die das nicht sind. Für die letzteren hat J selbst keine Bedeutung und erhält eine solche erst in der Integralrechnung, die der rein arithmetischen Methode nicht zugänglich ist.

Ist z eine beliebige Variable in Ω und dJ ein Differential, so ist $dJ:dz$ eine Funktion in α, und $dJ:dz$ ist ein Differentialquotient. Wir unterscheiden auch hier eigentliche und uneigentliche Differentialquotienten. Der Quotient zweier Differentiale $dJ:dJ'$ ist gleichfalls immer eine Funktion in Ω und kann ebenfalls ein Differentialquotient genannt werden.

Damit ein Polygonquotient $\mathfrak{A}:\mathfrak{B}$ das Symbol für ein Differential sein kann, ist notwendig, daß die Differenz $(a - b)$ der Ordnungen von $\mathfrak{A}$ und $\mathfrak{B}$ gleich $(2p - 2)$ sei. Aber diese Bedingung ist nicht hinreichend; es kommt noch hinzu, daß eine Variable z in Ω existieren muß, für die

(6) $$\mathfrak{U}^2\mathfrak{A} \sim \mathfrak{Z}\mathfrak{B}$$

ist. Ist diese Forderung befriedigt, so bleibt sie erhalten, wenn z durch irgend eine andere Variable in Ω und $\mathfrak{A}$ und $\mathfrak{B}$ durch äquivalente Polygone ersetzt werden. Sind also $\mathfrak{A}', \mathfrak{A}'', \ldots$ Polygone der durch $\mathfrak{A}$ bestimmten Klasse A, so sind $\mathfrak{A}':\mathfrak{B}, \mathfrak{A}'':\mathfrak{B}, \ldots$ gleichfalls Differentiale.

Ist
$$A = (\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \ldots)$$
und $\mathfrak{A}_1, \mathfrak{A}_2, \mathfrak{A}_3, \ldots$ eine Basis von A, so sind die entsprechenden Differentialquotienten
$$\frac{dJ_1}{dz}, \quad \frac{dJ_2}{dz}, \quad \frac{dJ_3}{dz}, \quad \ldots$$
die Basis einer Funktionenschar von endlicher Dimension, und wir können
$$(dJ_1, dJ_2, dJ_3, \ldots)$$
die Basis einer Schar von Differentialen von derselben Dimension nennen.

Jedes Differential dJ, dessen Untereck 𝔙 oder ein Teiler von 𝔙 ist, kann dann in der Form dargestellt werden:

(7) $$dJ = c_1 dJ_1 + c_2 dJ_2 + c_3 dJ_3 + \cdots$$

mit konstanten Koeffizienten.

Die einfachsten Differentiale sind die, deren Untereck das Nulleck ist, und deren Oberecke 𝔚 also von der Ordnung $(2p - 2)$ sind. Diese heißen Differentiale erster Gattung und werden mit dW bezeichnet. Sie sind dadurch charakterisiert, daß für jede Variable z die Polygone $\mathfrak{U}^2\mathfrak{W}$ und $\mathfrak{Z}$ äquivalent sein müssen, und die 𝔚 bilden also, ihre Existenz vorausgesetzt, eine Polygonklasse W, deren Dimension zu bestimmen ist.

Das Polygon 𝔚 heißt das Grundpolygon des Differentials dW und wird ein vollständiges Polygon erster Gattung genannt. Ist $\mathfrak{W} = \mathfrak{A}\mathfrak{B}$, so heißen auch 𝔄 und 𝔅 Polygone erster Gattung und zwar Ergänzungspolygone voneinander.

Jedes Polygon, das nicht Teiler eines vollständigen Polygons erster Gattung ist, heißt von der zweiten Gattung.

Ist 𝔄 ein Polygon erster Gattung, so ist auch jedes mit 𝔄 äquivalente Polygon 𝔄′ von der ersten Gattung, und wir nennen die Klasse A von 𝔄 eine Klasse erster Gattung. Denn ist $\mathfrak{A}\mathfrak{B} = \mathfrak{W}$, so ist $AB = W$, wenn B die Klasse von 𝔅 ist, und es ist $\mathfrak{A}'\mathfrak{B} = \mathfrak{W}'$ mit 𝔚 äquivalent, also von der ersten Gattung.

Ist also q die Anzahl der linear unabhängigen Polygone erster Gattung, die durch ein Polygon der Klasse A teilbar sind, so ist nach § 192, (14)

(8) $$q = (A, W) = (O, B),$$

also gleich der Dimension der Ergänzungsklasse.

Ist A eine Klasse zweiter Gattung, so gibt es kein durch 𝔄 teilbares Polygon erster Gattung, und es ist

$$(A, W) = 0.$$

§ 198. Die Polygonschar erster Gattung.

Um die Dimension (O, W) der Polygonschar erster Gattung zu bestimmen und damit zugleich ihre Existenz nachzuweisen, nehmen wir eine beliebige Variable z in Ω mit dem Verzweigungseck $\mathfrak{Z}$ und dem Untereck 𝔘. Ist dW ein Differential erster Gattung, so ist

(1) $$w = \frac{dW}{dz} = \frac{\mathfrak{W}\mathfrak{U}^2}{\mathfrak{Z}}$$

eine Funktion in Ω, die wir einen Differentialquotienten erster Gattung nennen.

Ist $\mathfrak{P}$ ein Punkt, in dem $(z - z_0)$ unendlich klein von der Ordnung e wird, so kommt dieser Punkt $(e - 1)$ mal in $\mathfrak{Z}$ vor, und folglich ist $[w(z - z_0)]_0 = 0$. Wird z in einem anderen Punkte $\mathfrak{P}$ unendlich in der $e$ten Ordnung, so kommt dieser Punkt e mal in $\mathfrak{U}$ und $(e - 1)$ mal in $\mathfrak{Z}$ vor, also einmal im Zähler von wz, und folglich ist auch in diesem Punkte $(wz)_0 = 0$, und diese beiden Forderungen, nämlich:

a) In jedem Punkte, in dem z einen endlichen Wert z_0 hat, ist $[w(z - z_0)]_0 = 0$;

b) In einem Punkte, in dem z unendlich wird, ist $(wz)_0 = 0$, sind auch ausreichend, einen Differentialquotienten erster Gattung w zu definieren.

Um die erste Bedingung zu erfüllen, nehmen wir eine Minimalbasis nach z:

(2) $$\omega_1, \omega_2, \ldots, \omega_n,$$

setzen

(3) $$a_{r,s} = S(\omega_r \omega_s),$$

so daß

(4) $$\Delta = \Sigma \pm a_{1,1}\, a_{2,2} \ldots a_{n,n}$$

die Körperdiskriminante (nach z) ist, und bestimmen eine Basis

(5) $$\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$$

aus den Gleichungen:

(6) $$\omega_r = \Sigma a_{r,i}\, \varepsilon_i.$$

Ist (r, s) ein Zeichen, das $= 0$ ist, wenn r und s verschieden sind, und $= 1$, wenn $r = s$ ist, so kann man die rationalen Funktionen $a'_{r,s}$ von z so bestimmen, daß

(7) $$\sum^{i} a_{i,r}\, a'_{i,s} = (r, s)$$

wird, und erhält aus (6):

(8) $$\varepsilon_r = \sum^{i} a'_{i,r}\, \omega_i,$$

und die Größen $a'_{r,s}$ haben keinen anderen Nenner als Δ. Daraus ergibt sich wegen (3) und (7):

(9) $$S(\varepsilon_r \omega_s) = (r, s), \quad a'_{r,s} = S(\varepsilon_r \varepsilon_s).$$

Ist umgekehrt für ein Funktionensystem $\eta_1, \eta_2, \ldots, \eta_n$ die Bedingung

(10) $$S(\eta_r \omega_s) = (r, s)$$

befriedigt, so ist $\eta_r = \varepsilon_r$; denn setzt man

$$\eta_r = \sum^i x_{i,r} \varepsilon_i,$$

so folgt aus (9) und (10) $x_{r,s} = (r, s)$. Demnach sind die Bedingungen (9) und (6) vollständig gleichbedeutend.

Die Größen ε_i bilden eine Basis von Ω, sind aber nicht ganze Funktionen. Die Basen (5) und (2) heißen zueinander komplementär.

Die Größen

(11) $$\Delta \varepsilon_1, \Delta \varepsilon_2, \ldots, \Delta \varepsilon_n$$

sind ganze Funktionen, und wenn $t_1, t_2, \ldots, t_n$ Funktionalvariablen sind, so ist

(12) $$\Delta(\varepsilon_1 t_1 + \varepsilon_2 t_2 + \cdots + \varepsilon_n t_n) = \Delta \varepsilon$$

der größte gemeinschaftliche Teiler der Funktionen (11).

Ist

(13) $$r = (z - c_1)(z - c_2)(z - c_3) \ldots$$

das Produkt aller voneinander verschiedenen Linearfaktoren von Δ und

(14) $$\varkappa = \pi_1 \pi_2 \pi_3 \ldots$$

das Produkt der verschieden in Δ aufgehenden Primfunktionale, so können wir jede durch r teilbare ganze Funktion ϱ von z in Ω in die Form setzen:

$$\varrho = r(x_1 \varepsilon_1 + x_2 \varepsilon_2 + \cdots + x_n \varepsilon_n),$$

worin die $x_1, x_2, \ldots, x_n$ rationale Funktionen von z sind. Dann erhält man nach (9)

$$r x_i = S(\varrho \omega_i),$$

und da $\varrho \omega_i$ durch jeden Primfaktor von r teilbar ist, so ist $S(\varrho \omega_i)$ nach dem Satz § 184, 7. eine durch r teilbare ganze Funktion in Z, und folglich x_i eine ganze rationale Funktion.

Hieraus folgt, daß

$$\Delta \varrho = r(x_1 \Delta \varepsilon_1 + x_2 \Delta \varepsilon_2 + \cdots + x_n \Delta \varepsilon_n)$$

durch $r \varepsilon \Delta$ teilbar ist, und daß sonach $r \varepsilon$ ein in ϱ aufgehendes ganzes Funktional ist.

Wäre π ein nicht in $\varkappa$ enthaltener Primfaktor von $r \varepsilon$, so könnte man ϱ so annehmen, daß es nicht durch π teilbar ist,

und ϱ könnte nicht durch $r\varepsilon$ teilbar sein. Ebenso schließt man, daß jeder der Primfaktoren $\pi_1, \pi_2, \ldots$, aber keiner mehr als einmal in $r\varepsilon$ aufgeht; also ist, von Einheitsfaktoren abgesehen,

$$r\varepsilon = \varkappa. \tag{15}$$

Also genügt jede der Funktionen $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ der Bedingung a). Umgekehrt ist auch jede dieser Bedingung genügende Funktion w in der Form enthalten:

$$w = x_1\varepsilon_1 + x_2\varepsilon_2 + \cdots + x_n\varepsilon_n, \tag{16}$$

worin die $x_1, x_2, \ldots, x_n$ ganze rationale Funktionen von z sind.

Denn es ist rw eine durch $\varkappa$ teilbare ganze Funktion, und folglich nach (9), (16) und § 184, 7.:

$$S(rw\omega_i) = rx_i$$

eine durch r teilbare ganze Funktion von z, folglich

$$x_i = S(w\omega_i). \tag{17}$$

Um also die Differentialquotienten erster Gattung zu erhalten, hat man unter den Funktionen (16) die auszusuchen, die der Bedingung b) genügen.

Zu dem Zweck nehmen wir für (2) die in § 193 betrachtete Normalbasis

$$\lambda_1, \lambda_2, \ldots, \lambda_n$$

und bezeichnen die dazu komplementäre Basis mit

$$\mu_1, \mu_2, \ldots, \mu_n,$$

die durch

$$S(\lambda_r\mu_s) = (r, s) \tag{18}$$

definiert ist.

Setzen wir dann

$$w = y_1\mu_1 + y_2\mu_2 + \cdots + y_n\mu_n, \tag{19}$$

so ist, wenn r_i der Exponent von λ_i ist, nach (17)

$$\frac{y_i}{z^{r_i-1}} = S\left(wz\frac{\lambda_i}{z^{r_i}}\right).$$

Nach der Definition von r_i ist $\lambda_i : z^{r_i}$ für $z = \infty$ endlich und wz verschwindet wegen b). Folglich muß $y_i : z^{r_i-1}$ für $z = \infty$ verschwinden, d. h. y_i kann höchstens vom Grade $(r_i - 2)$ sein und enthält daher höchstens $r_i - 1$ konstante Koeffizienten.

Da $\mu_1 = 1$, $r_1 = 0$ ist und der Grad von y_1 nicht negativ sein kann, so muß y_1 identisch Null sein und es folgt

$$S(w) = 0.$$

Dies ist das Abelsche Theorem für die Differentialquotienten erster Gattung.

Um zu zeigen, daß diese Forderung über die y_i für die Erfüllung von b) auch genügt, betrachten wir die Funktionen in Ω als Funktionen von $z' = 1:z$. Für diese bildet

$$\lambda_1' = z'^{r_1}\lambda_1,\ \lambda_2' = z'^{r_2}\lambda_2,\ \ldots,\ \lambda_n' = z'^{r_n}\lambda_n$$

nach § 193, 6. eine Minimalbasis, und

$$\mu_1' = z^{r_1}\mu_1,\ \mu_2' = z^{r_2}\mu_2,\ \ldots,\ \mu_n' = z^{r_n}\mu_n$$

ist nach (10) die dazu komplementäre Basis. Folglich ist $z'\mu' = 0$ für $z' = 0$ [nach a), auf z' angewandt], also

$$z^{r_i-1}\mu_i = 0,$$

$$z y_i \mu_i = \frac{y_i}{z^{r_i-2}} z^{r_i-1}\mu_i = 0 \text{ für } z = \infty,$$

wenn der Grad von y_i nicht höher als $(r_i - 1)$ ist.

Damit ist nachgewiesen, daß alle in der Form (19) enthaltenen Funktionen, in denen die y_i ganze rationale Funktionen von z, höchstens vom Grade $r_i - 2$ sind, Differentialquotienten erster Gattung sind, und daß auch umgekehrt in dieser Form alle Differentialquotienten erster Gattung darstellbar sind, und es folgt der Hauptsatz:

1. Die Klasse der Differentiale erster Gattung ist von der Dimension

$$(O, W) = (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1) = p.$$

Hieraus ergibt sich noch folgendes: Ist A eine beliebige Polygonklasse von der Ordnung a und W die Hauptklasse erster Gattung, so ist nach § 192, (14):

$$(A, W) \gtreqless (O, W) - a = p - a,$$

also, wenn $a \lesseqgtr p - 1$ ist:

$$(A, W) \gtreqless 1.$$

Es gibt also, wenn a kleiner als p ist, immer Polygone erster Gattung, die durch $\mathfrak{A}$ teilbar sind, und daraus folgt:

2. Jedes Polygon von $(p-1)$ter und niedrigerer Ordnung ist von der ersten Gattung.

Nach § 192, 5. kann man, wenn m nicht größer als p ist, ein m-Eck $\mathfrak{M}$ so wählen, daß, wenn M die durch $\mathfrak{M}$ bestimmte Klasse ist,

$$(M, W) = p - m$$

wird, und wenn man hier $m = p$ setzt, so folgt, daß es Klassen der Ordnung p von der zweiten Gattung gibt.

§ 199. Der Riemann-Rochsche Satz.

Das unter dem Namen des Riemann-Rochschen Satzes bekannte Theorem hat den Zweck, die Dimensionen von Polygonklassen zu bestimmen.

Wir betrachten zunächst eine eigentliche Polygonklasse A von der Ordnung n, nehmen darin zwei teilerfremde Polygone $\mathfrak{A}$, $\mathfrak{A}'$ und setzen:

$$z = \frac{\mathfrak{A}'}{\mathfrak{A}}.$$

Ist dann $\mathfrak{A}''$ ein anderes Polygon derselben Klasse, so setzen wir

$$\omega = \frac{\mathfrak{A}''}{\mathfrak{A}}, \quad \frac{\omega}{z} = \frac{\mathfrak{A}''}{\mathfrak{A}'}.$$

Es ist also ω eine ganze Funktion von z, und $\omega : z$ eine ganze Funktion von $1 : z$. Wenn also ω nicht konstant ist, so ist der Exponent r von ω gleich 1. Umgekehrt ist auch jede ganze Funktion ω von z vom Exponenten 0 oder 1 in der Form $\mathfrak{A}'' : \mathfrak{A}$ darstellbar.

Wir erhalten also die ganze Klasse A aus der Gesamtheit der ganzen Funktionen von z, deren Exponent $\lesseqgtr 1$ ist. Diese erhalten wir aber leicht aus der Normalbasis $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ in z, mit der Reihe der Exponenten $r_1, r_2, \ldots, r_n$ (§ 193). Ist λ_s die letzte dieser Funktionen, deren Exponent gleich 1 oder 0 ist, so ist jede ganze Funktion, deren Exponent $\lesseqgtr 1$ ist, in der Form

(1) $$\omega = c_0 z + c_1 \lambda_1 + c_2 \lambda_2 + \cdots + c_s \lambda_s$$

darstellbar (c_0 muß konstant sein, weil es nach der Definition der Normalbasis eine ganze Funktion sein muß, und wenn sein Exponent positiv wäre, so wäre der Exponent von ω größer als eins). Demnach ist

(2) $$(O, A) = s + 1,$$

und diese Zahl ist also immer $\lesseqgtr n + 1$.

Die obere Grenze $n + 1$ wird nur dann erreicht, wenn alle $r_2, r_3, \ldots, r_n = 1$ und folglich $p = 0$ ist.

Da in einer eigentlichen Klasse mindestens zwei Polygone enthalten sind, also $(O, A) \gtreqless 2$ sein muß, so kann $n = 1$ nur in dem Falle $p = 0$ vorkommen.

Eine Funktion z, die nur in je einem Punkte 0 und ∞ wird, also die Ordnung 1 hat, gibt es daher nur in dem Falle $p = 0$. Jede Funktion in Ω ist durch ein solches z rational darstellbar[1]).

Wenn $r_i > 2$ ist, so sind μ_i und $z\mu_i$ nach § 198 Differentialquotienten erster Gattung. Es gibt also nach (1) Polygone $\mathfrak{W}$, $\mathfrak{W}'$ von der ersten Gattung, die der Bedingung genügen:

$$\mu_i = \frac{\mathfrak{A}^2\mathfrak{W}}{\mathfrak{Z}}, \quad \mu_i z = \frac{\mathfrak{A}^2\mathfrak{W}'}{\mathfrak{Z}}, \quad z = \frac{\mathfrak{W}'}{\mathfrak{W}} = \frac{\mathfrak{A}'}{\mathfrak{A}},$$

und da $\mathfrak{A}$, $\mathfrak{A}'$ teilerfremd sind, so muß $\mathfrak{A}$ in $\mathfrak{W}$, $\mathfrak{A}'$ in $\mathfrak{W}'$ aufgehen. Es ist also A eine Klasse erster Gattung.

Ist A eine Klasse zweiter Gattung, so sind also alle Exponenten $r_1, r_2, \ldots, r_n$ gleich 2 oder kleiner als 2, und es ist im besonderen $r_{s+1} = 2$, $r_{s+2} = 2, \ldots, r_n = 2$. Folglich ist

$$p = (r_2 - 1) + (r_3 - 1) + \cdots + (r_n - 1) = n - s,$$

und wir haben nach (2) den Satz:

3. Die Dimension einer eigentlichen Klasse A von der zweiten Gattung ist

$$(O, A) = n - p + 1. \tag{3}$$

Ist ferner A eine eigentliche Klasse erster Gattung und

$$AB = W \tag{4}$$

die vollständige Klasse erster Gattung, so nehme man ein Polygon $\mathfrak{B}$ in B und bilde die Differentialquotienten erster Gattung:

$$w = \frac{\mathfrak{A}^3\mathfrak{B}}{\mathfrak{Z}}, \quad zw = \frac{\mathfrak{A}^2\mathfrak{A}'\mathfrak{B}}{\mathfrak{Z}},$$

und diese Form bleibt erhalten, wenn $\mathfrak{B}$ durch ein äquivalentes Polygon $\mathfrak{B}'$ ersetzt wird. Die Dimension (O, B) ist also so groß wie die Dimension der Schar der Differentialquotienten erster Gattung w, die die Eigenschaft haben, daß auch zw noch von der ersten Gattung ist. Damit dies der Fall sei, dürfen in dem Ausdruck:

$$w = y_1\mu_1 + y_2\mu_2 + \cdots + y_n\mu_n$$

die Grade der Funktionen $y_1, y_2, \ldots, y_n$ nur bis zu der Höhe $r_1 - 2, r_2 - 2, \ldots, r_n - 2$, ansteigen, und daraus folgt:

---

[1]) Dieser Funktionenkörper führt zu den von den Geometern so genannten „Unikursalkurven".

$$(5)\quad \begin{aligned} (O, B) &= (r_{s+1} - 2) + (r_{s+2} - 2) + \cdots + (r_n - 2), \\ p &= (r_{s+1} - 1) + (r_{s+2} - 1) + \cdots + (r_n - 1), \\ (O, B) &= p - n + s, \end{aligned}$$

und nach (2):

$$(O, A) - (O, B) = n - p + 1.$$

Nun ist nach § 192, (14) $(O, B) = (A, W)$, und wir haben den Riemann-Rochschen Satz für Klassen erster Gattung:

4. Die Dimension einer eigentlichen Klasse A erster Gattung ist

$$(6)\qquad (O, A) = n - p + 1 + (A, W).$$

Diese Formel schließt (3) in sich, weil für Polygone zweiter Gattung $(A, W) = 0$ ist.

Da die Dimension einer eigentlichen Klasse mindestens gleich 2 ist, so folgt für eine Klasse zweiter Gattung:

$$n \gtreqless p + 1,$$

und hierin ist der Beweis eines Satzes von Riemann enthalten:

5. Eine Funktion, deren Ordnung kleiner als $(p + 1)$ ist, ist von der ersten Gattung.

Es folgt weiter daraus, daß die Klasse W der Polygone erster Gattung eine eigentliche ist. Denn angenommen, W habe den Teiler $\mathfrak{M}$, und es sei $W = \mathfrak{M} A$, so wäre $(O, W) = (O, A) = p$. Nimmt man $\mathfrak{A}$ in A relativ prim zu $\mathfrak{M}$, so gibt es in W nur ein durch $\mathfrak{A}$ teilbares Polygon, nämlich $\mathfrak{A}\mathfrak{M}$, und folglich ist $(A, W) = 1$. Demnach gibt die Formel (6):

$$n = 2p - 2,$$

also gleich der Ordnung von W. Die Ordnung von A ist also ebenso groß wie die von W, und folglich $\mathfrak{M} = \mathfrak{O}$.

Der Satz 4. gilt unverändert auch für uneigentliche Klassen. Um das nachzuweisen, sei zunächst A von der ersten Gattung und vom Teiler $\mathfrak{M}$:

$$(7)\quad \begin{aligned} A &= \mathfrak{M} A', \\ AB &= W, \\ A'B' &= W, \\ B' &= \mathfrak{M} B, \qquad (\S\ 192,\ 8.) \\ (A', W) &= (O, B'). \end{aligned}$$

Die Ordnungen von $\mathfrak{M}$, A, B seien m, a, b, also $a + b$ die Ordnung von W, d. h.

$$(8)\qquad a + b = 2(p - 1).$$

Nach (7) und § 192 ist

(9) $$(O, B) \gtreqless (O, B') - m,$$

und nach (6), angewandt auf A':

$$(O, A) = (O, A') = a - m - p + 1 + (O, B'),$$

also nach (8):

$$(O, A) - \tfrac{1}{2}a \lesseqgtr (O, B) - \tfrac{1}{2}b.$$

Da wir aber A und B vertauschen können, so ergibt sich hieraus

$$(O, A) - \tfrac{1}{2}a = (O, B) - \tfrac{1}{2}b,$$

und wenn man

$$(O, B) = (A, W),$$
$$\tfrac{1}{2}(a - b) = a - p + 1$$

setzt:

$$(O, A) = a - p + 1 + (A, W)$$

in genauer Übereinstimmung mit (6).

Um auch für uneigentliche Klassen zweiter Gattung den entsprechenden Satz abzuleiten, sei

(10) $$A = \mathfrak{M} A'$$

eine uneigentliche Klasse zweiter Gattung vom Teiler $\mathfrak{M}$.

In einer eigentlichen Klasse zweiter Gattung, C, deren Dimension größer ist als die Ordnung a von A, gibt es nach § 192, 5. immer Polygone, die durch ein Polygon der Klasse A teilbar sind, und C ist also auch durch A teilbar.

Aus § 192, (15) folgt:

$$(O, A) \gtreqless (O, C) - c + a,$$

und aus (3):

$$(O, C) = c - p + 1,$$

also

(11) $$(O, A) \gtreqless a - p + 1.$$

Nun ist A' eine eigentliche Klasse von derselben Dimension wie A, also, wenn m die Ordnung von $\mathfrak{M}$ ist, nach (6):

(12) $$(O, A) = (O, A') = a - m - p + 1 + (A', W),$$

also nach (11):

(13) $$(A', W) \gtreqless m.$$

Daraus folgt, daß A' von der ersten Gattung sein muß.

Ist $W = A'B'$, so folgt aus (13):

(14) $$(A', W) = (O, B') \gtreqless m.$$

Wäre nun $(O, B') > m$, so könnte man in B' ein durch $\mathfrak{M}$ teilbares Polygon $\mathfrak{M}\mathfrak{B}$ finden (§ 192, 5.), und es wäre:

$$\mathfrak{A}'\mathfrak{M}\mathfrak{B} = \mathfrak{A}\mathfrak{B} = \mathfrak{W}$$

ein vollständiges Polygon erster Gattung, es wäre also $\mathfrak{A}$ selbst von der ersten Gattung; gegen die Voraussetzung. Also ist $(O, B') = (A', W) = m$ und

$$(15) \qquad (O, A) = a - p + 1.$$

Also gilt auch hier der Riemann-Rochsche Satz in der Form 3.

Besteht A aus einem isolierten Polygon $\mathfrak{M}$, so ist $(O, A) = 1$, also $a = p$, und daraus folgt:

6. Ein isoliertes Polygon zweiter Gattung muß ein p-Eck sein, und umgekehrt ist jedes p-Eck zweiter Gattung ein isoliertes Polygon.

7. Geht ein Punkt $\mathfrak{P}$ im Teiler einer uneigentlichen Klasse zweiter Gattung A auf, und ist $A = \mathfrak{P}A'$, so muß A' von der ersten Gattung sein.

Denn es ist nach dem Satz (6) und (15):

$$(O, A) = a - p + 1,$$
$$(O, A') = a - p + (A', W),$$
$$(O, A) = (O, A'),$$

also $(A', W) = 1$.

§ 200. Differentiale zweiter und dritter Gattung.

Wir können jetzt die Bedingung für ein Differential:

$$(1) \qquad dJ = \frac{\mathfrak{A}}{\mathfrak{B}},$$

die wir in § 197, (6) mit Rücksicht auf eine Variable z in der Form ausgedrückt haben:

$$\mathfrak{U}^2\mathfrak{A} \sim \mathfrak{Z}\mathfrak{B},$$

invariant darstellen, wenn wir die vollständigen Polygone erster Gattung benutzen, wonach

$$\mathfrak{U}^2\mathfrak{W} \sim \mathfrak{Z}$$

ist:

$$\mathfrak{A} \sim \mathfrak{W}\mathfrak{B},$$

oder, indem wir die Klassen einführen:

1. Der Polygonquotient (1) ist ein Differential, wenn die Klassen A, B von $\mathfrak{A}$ und $\mathfrak{B}$ relativ prim sind und der Bedingung genügen:

(2) $$A = WB.$$

Sind a und b die Ordnungszahlen von A und B, so ist:

(3) $$a - b = 2p - 2,$$

und da A jedenfalls von der zweiten Gattung ist, nach § 199, (15):

(4) $$(O, A) = b + p - 1.$$

Besteht B aus einem einzelnen Punkt $\mathfrak{P}$, so ist $(O, A) = p$, und die Dimension von A ist ebenso groß wie die von W; ist daher

$$(\mathfrak{W}_1, \mathfrak{W}_2, \ldots, \mathfrak{W}_p)$$

eine Basis von W, so ist

$$(\mathfrak{P}\mathfrak{W}_1, \mathfrak{P}\mathfrak{W}_2, \ldots, \mathfrak{P}\mathfrak{W}_p)$$

eine Basis von A. Daher ist A eine uneigentliche Klasse mit dem Teiler $\mathfrak{P}$, und es folgt:

2. Ein einzelner Punkt $\mathfrak{P}$ kann nicht Untereck eines Differentials sein.

Hat die Klasse A einen Teiler $\mathfrak{M}$ vom Grade m, so muß $\mathfrak{M}$ im Teiler von B enthalten sein; denn $\mathfrak{M}$ muß in jedem der Polygone $\mathfrak{W}\mathfrak{B}$, und folglich, da W eine eigentliche Klasse ist, in jedem der $\mathfrak{B}$ aufgehen. Ist

$$\mathfrak{M}A' = A, \quad \mathfrak{M}B' = B,$$

so muß

(5) $$(O, A) = (O, A')$$

sein. Es ist aber nach (3) und (4), auf A und A' angewandt, wenn A' von der zweiten Gattung ist:

$$(O, A) = (O, A') + m,$$

also $(O, A) > (O, A')$; folglich muß $m = 0$ sein.

A' kann aber nur dann von der ersten Gattung sein, wenn B ein isoliertes Polygon und $B = \mathfrak{M}$ ist. Dann ist:

$$A' = W, \quad (O, A') = p,$$

also muß $(O, A) = p$, $b = 1$ sein, und wir kommen auf den Fall des Satzes 2. Folglich:

3. Jedes Polygon von mehr als einem Punkt kann Untereck eines Differentials sein.

Unter einem Differential zweiter Gattung versteht man ein solches, dessen Untereck eine Potenz eines einzelnen Punktes $\mathfrak{P}$

ist. Ein Differential, dessen Untereck nur aus zwei einfachen Punkten besteht, heißt ein Differential dritter Gattung. Wir beweisen den Satz:

4. Jedes Differential dJ läßt sich linear und mit konstanten Koeffizienten aus Differentialen erster, zweiter und dritter Gattung zusammensetzen.

Dieser Satz kann nach (4) auch so ausgesprochen werden, daß die Klasse A eine Basis

(6) $$\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_{b+p-1}$$

von der Art hat, daß die Quotienten

(7) $$d J_r = \frac{\mathfrak{A}_r}{\mathfrak{B}}$$

Differentiale von einer der drei Gattungen sind.

Um ihn durch vollständige Induktion zu beweisen, nehmen wir an, es sei für irgend ein $\mathfrak{B}$ eine solche Basis gefunden, und suchen eine ebensolche für das Untereck $\mathfrak{P}\mathfrak{B}$, wenn $\mathfrak{P}$ ein beliebiger Punkt ist. Eine solche Basis können wir in der Form annehmen:

(8) $$\mathfrak{P}\mathfrak{A}_1, \mathfrak{P}\mathfrak{A}_2, \ldots, \mathfrak{P}\mathfrak{A}_{b+p-1}, \mathfrak{A}_{b+p},$$

worin $\mathfrak{A}_{b+p}$ ein mit $\mathfrak{W}\mathfrak{B}\mathfrak{P}$ äquivalentes Polygon sein muß, das den Punkt $\mathfrak{P}$ nicht enthält.

Wenn der Punkt $\mathfrak{P}$ in $\mathfrak{B}$ aufgeht, setzen wir:

$$\mathfrak{B} = \mathfrak{M}\mathfrak{P}^m,$$

so daß $\mathfrak{P}$ nicht mehr in $\mathfrak{M}$ aufgeht. Das Polygon $\mathfrak{W}\mathfrak{P}^{m+1}$ gehört dann in eine eigentliche Klasse, in der also ein durch $\mathfrak{P}$ nicht teilbares Polygon $\mathfrak{N}$ existiert.

Wir setzen dann:

$$\mathfrak{A}_{b+p} = \mathfrak{M}\mathfrak{N},$$

und erhalten daraus ein Differential zweiter Gattung:

(9) $$d J_{b+p} = \frac{\mathfrak{A}_{b+p}}{\mathfrak{B}\mathfrak{P}} = \frac{\mathfrak{N}}{\mathfrak{P}^{m+1}}.$$

Geht $\mathfrak{P}$ in $\mathfrak{B}$ nicht auf, so nehme man einen in $\mathfrak{B}$ aufgehenden Punkt $\mathfrak{P}_0$. Dann gehört $\mathfrak{W}\mathfrak{P}_0\mathfrak{P}$ in eine eigentliche Klasse und enthält ein durch $\mathfrak{P}$ nicht teilbares Polygon $\mathfrak{N}$. Ist dann

$$\mathfrak{B} = \mathfrak{P}_0\mathfrak{M}, \quad \mathfrak{A}_{b+p} = \mathfrak{M}\mathfrak{N},$$

so ist

(10) $$d J_{b+p} = \frac{\mathfrak{A}_{b+p}}{\mathfrak{B}\mathfrak{P}} = \frac{\mathfrak{N}}{\mathfrak{P}_0\mathfrak{P}}$$

ein Differential dritter Gattung. Damit ist der Satz 4. bewiesen, sogar mit der Verschärfung, daß die darin auftretenden Differentiale dritter Gattung einen beliebigen festen Punkt $\mathfrak{P}_0$ im Untereck enthalten.

§ 201. Die Residuen.

Ist $\mathfrak{P}$ ein Punkt, der m mal im Untereck $\mathfrak{B}$ eines Differentials dJ aufgeht ($m \gtreqless 0$), so nehme man eine Funktion z in Ω, die in $\mathfrak{P}$ unendlich groß in der ersten Ordnung wird. Dann kann man nach § 197, (1) und § 185, (5) setzen:

$$(1)\quad \frac{dJ}{dz} = a_{m-2} z^{m-2} + a_{m-3} z^{m-3} + \cdots + a_0 + a_{-1} z^{-1} + \eta z^{-2},$$

worin die a Konstanten sind, η eine in $\mathfrak{P}$ endliche Funktion in Ω.

Der Koeffizient $-a_{-1}$ von $-z^{-1}$ heißt das Residuum des Differentials dJ in bezug auf den Punkt $\mathfrak{P}$.

Das Residuum von dJ im Punkt $\mathfrak{P}$ kann nur dann von Null verschieden sein, wenn $m > 0$ ist, d. h. wenn der Punkt $\mathfrak{P}$ im Untereck von dJ vorkommt. Solche Punkte sollen Pole von dJ heißen.

1. Das Residuum eines eigentlichen Differentials ist gleich Null. Denn durch Differentiation einer Potenz von z kann niemals z^{-1} entstehen.

Nimmt man für z eine Funktion z_1, die gleichfalls in $\mathfrak{P}$ unendlich von der ersten Ordnung wird, so kann man setzen:

$$(2)\quad \begin{gathered} z = c z_1 + \eta_1, \quad z^{-1} = c^{-1} z_1^{-1} + \eta_2, \\ \frac{dz}{dz_1} = c + z_1^{-2} \eta_3, \end{gathered}$$

worin die c Konstanten, η_1, η_2, η_3, in $\mathfrak{P}$ endlich sind.

Setzt man

$$\frac{a_{m-2} z^{m-1}}{m-1} + \frac{a_{m-3} z^{m-2}}{m-2} + \cdots + a_0 = \omega,$$

so ergibt sich aus (1):

$$\frac{dJ}{dz_1} = \frac{d\omega}{dz_1} + a_{-1} z^{-1} \frac{dz}{dz_1} + z^{-2} \eta',$$

wo η' in $\mathfrak{P}$ endlich bleibt, und darin gibt nach 1. nur der Teil

$$a_{-1} z^{-1} \frac{dz}{dz_1}$$

einen Beitrag zu dem Gliede mit z_1^{-1}, und dieser hat nach (2) den Koeffizienten a_{-1}. Daraus folgt:

2. Das Residuum von dJ ist von der Wahl der Funktion z unabhängig.

Es gilt ferner noch der folgende Satz:

3. Die Summe aller Residuen eines Differentials ist gleich Null.

Wir erweitern den Ausdruck $\mathfrak{A}/\mathfrak{B}$ des Differentials dJ, wenn nötig, durch Hinzufügung von Punkten im Zähler und Nenner, so daß die voneinander verschiedenen Punkte des Unterecks

$$(3) \qquad \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_n$$

ein Polygon einer eigentlichen Klasse bilden. Die Pole von dJ sind dann unter diesen $\mathfrak{P}$ enthalten, möglicherweise auch noch andere Punkte, für die das Residuum von dJ gleich Null ist.

Als Nenner von dJ können wir dann

$$(4) \qquad \mathfrak{B} = \mathfrak{P}_1^{m_1} \mathfrak{P}_2^{m_2} \ldots \mathfrak{P}_n^{m_n}$$

nehmen, wenn wir die zuviel genommenen Punkte wieder im Zähler zufügen.

Wir nehmen eine Funktion z in Ω von der $n$ten Ordnung, die in jedem der Punkte $\mathfrak{P}_i$ und in jedem nur zur ersten Ordnung unendlich wird, und bilden die Entwickelung für den Punkt $\mathfrak{P}_i$:

$$(5) \qquad \frac{dJ}{dz} = a_{m-2}^{(i)} z^{m-2} + \cdots + a_0^{(i)} + a_{-1}^{(i)} z^{-1} + \eta^{(i)} z^{-2}.$$

Wenn wir für den Koeffizienten $a_r^{(i)}$ den Wert 0 zulassen, können wir in allen Punkten $\mathfrak{P}_i$ mit derselben Potenz z^{m-2} anfangen. Die Summe der Residuen von dJ ist

$$-\sum^{i} a_{-1}^{(i)}.$$

Nach § 182, 11. läßt sich ein Funktionensystem $\alpha_1, \alpha_2, \ldots, \alpha_n$ so bestimmen, daß α_r in dem Punkte $\mathfrak{P}_r$ unendlich klein in der ersten Ordnung wird, in den übrigen Punkten $\mathfrak{P}_i$ endlich und von Null verschieden bleibt.

Setzt man dann

$$\alpha_1^m \alpha_2^m \ldots \alpha_n^m = \alpha_i^m \varrho_i,$$

so wird

$$(6) \qquad \begin{array}{llll} \varrho_1 = 0^m & \text{in } \mathfrak{P}_2, \mathfrak{P}_3, \ldots, \mathfrak{P}_n, & \text{endlich und nicht} & = 0 \text{ in } \mathfrak{P}_1, \\ \varrho_2 = 0^m & \text{„ } \mathfrak{P}_1, \mathfrak{P}_3, \ldots, \mathfrak{P}_n, & \text{„ „ „} & = 0 \text{ „ } \mathfrak{P}_2, \\ \ldots & \ldots & \ldots & \ldots \\ \varrho_n = 0^m & \text{„ } \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_{n-1} & \text{„ „ „} & = 0 \text{ in } \mathfrak{P}_n. \end{array}$$

Verstehen wir nun unter $x_1, x_2, \ldots, x_n$ rationale Funktionen von z, die nicht alle identisch $= 0$ sind, und setzen:

$$(7) \qquad \eta = x_1 \varrho_1 + x_2 \varrho_2 + \cdots + x_n \varrho_n,$$

so kann η nur dann für $z = \infty$, d. h. in den Punkten $\mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_n$ endlich sein, wenn die x_i für $z = \infty$ endlich bleiben, also Brüche sind, deren Zähler nicht von höherem Grade ist als der Nenner.

Sind nämlich die $x_1, x_2, \ldots, x_n$ für $z = \infty$ nicht alle endlich, so gibt es einen positiven Exponenten r, so daß die Produkte $x_1 z^{-r}, x_2 z^{-r}, \ldots, x_n z^{-r}$ für $z = \infty$ endlich sind, und mindestens eines dieser Produkte, etwa $x_1 z^{-r}$, von Null verschieden. Dann ist

$$z^{-r} \eta = x_1 z^{-r} \varrho_1 + x_2 z^{-r} \varrho_2 + \cdots + x_n z^{-r} \varrho_n$$

im Punkte $\mathfrak{P}_1$ endlich und von Null verschieden, und η kann daher in $\mathfrak{P}_1$ nicht endlich sein. Ebenso sieht man, daß keine Relation von der Form

$$x_1 \varrho_1 + x_2 \varrho_2 + \cdots + x_n \varrho_n = 0$$

bestehen kann, d. h. die $\varrho_1, \varrho_2, \ldots, \varrho_n$ bilden eine Basis nach z.

Setzen wir also

$$(8) \qquad \varrho_i \frac{dJ}{dz} = x_{i,1} \varrho_1 + x_{i,2} \varrho_2 + \cdots + x_{i,n} \varrho_n,$$

so ist

$$(9) \qquad S\left(\frac{dJ}{dz}\right) = x_{1,1} + x_{2,2} + \cdots + x_{n,n}.$$

Nach (5) ist

$$z^{-m+2} \frac{dJ}{dz} \varrho_i$$

für $z = \infty$ endlich und folglich gilt das gleiche von

$$(10) \qquad z^{-m+2} x_{i,1}, \quad x^{-m+2} x_{i,2}, \quad \ldots, \quad z^{-m+2} x_{i,n}.$$

Es enthalten also die Funktionen $z x_{r,s}$ jeden der Punkte $\mathfrak{P}$ höchstens $m - 1$ mal im Nenner, und

$$z \frac{dJ}{dz} \varrho_1$$

enthält jeden der Punkte $\mathfrak{P}_2, \mathfrak{P}_3, \ldots$ im Zähler. ($\mathfrak{P}_1$ im allgemeinen nicht.)

Nun ist nach (8):

$$z \frac{dJ}{dz} \varrho_1 = z x_{1,1} \varrho_1 + z x_{1,2} \varrho_2 + \cdots + z x_{1,n} \varrho_n.$$

Diese Funktion muß also in $\mathfrak{P}_2, \mathfrak{P}_3, \ldots$ verschwinden. In dem Punkte $\mathfrak{P}_2$ verschwindet aber $z x_{1,1} \varrho_1$, $z x_{1,3} \varrho_3, \ldots, z x_{1,n} \varrho_n$, während ϱ_2 nicht verschwindet. Folglich muß $z x_{1,2}$ in $\mathfrak{P}_2$, d. h. für $z = \infty$, verschwinden und $z^2 x_{1,2}$ endlich bleiben. Wir haben also:

Ist r nicht gleich s, so ist $z^2 x_{r,s}$ für $z = \infty$ endlich.

Wir definieren nun die rationale Funktion $u^{(i)}$ durch:

$$(11)\quad x_{i,i} = a_{m-2}^{(i)} z^{m-2} + a_{m-3}^{(i)} z^{m-3} + \cdots + a_{-1}^{(i)} z^{-1} + u^{(i)} z^{-2},$$

worin die Konstante $a_\nu^{(i)}$ dieselbe sein soll wie in (5), und wir erhalten:

$$(12)\quad \frac{dJ}{dz} - x_{i,i} = z^{-2}[\eta^{(i)} - u^{(i)}],$$

und nach (8):

$$[\eta^{(i)} - u^{(i)}]\varrho_i = z^2 x_{i,1}\varrho_1 + \cdots + z^2 x_{i,i-1}\varrho_{i-1} + z^2 x_{i,i+1}\varrho_{i+1} + \cdots + z^2 x_{i,n}\varrho_n.$$

Im Punkte $\mathfrak{P}_i$ ist $\eta^{(i)}$ endlich und ϱ_i von Null verschieden, während auf der rechten Seite alles in $\mathfrak{P}_i$ verschwindet. Folglich muß auch $u^{(i)}$ in $\mathfrak{P}_i$, und, weil es rational ist, für $z = \infty$ endlich sein, und aus (9) und (11) folgt:

$$(13)\quad S\left(\frac{dJ}{dz}\right) = \sum^i a_{m-2}^{(i)} z^{m-2} + \cdots + \sum^i a_{-1}^{(i)} z^{-1} + \sum^i u^{(i)} z^{-2}.$$

Nach unserer Annahme über z enthält das Untereck $\mathfrak{B}$ von dJ keinen Punkt, in dem z einen endlichen Wert hat.

Ist $\mathfrak{P}$ ein Punkt, in dem z den endlichen Wert z_0 hat, so ist

$$(14)\quad (z - z_0) = \frac{\mathfrak{N}}{\mathfrak{U}},\quad \frac{dJ}{dz} = \frac{\mathfrak{A}\,\mathfrak{U}^2}{\mathfrak{Z}\,\mathfrak{B}},\quad (z - z_0)\frac{dJ}{dz} = \frac{\mathfrak{U}\,\mathfrak{N}\,\mathfrak{A}}{\mathfrak{Z}\,\mathfrak{B}},$$

und in $\mathfrak{N}$ ist der Punkt $\mathfrak{P}$ einmal öfter enthalten als in $\mathfrak{Z}$, folglich ist:

$$(15)\quad \left[(z - z_0)\frac{dJ}{dz}\right]_0 = 0 \text{ (in } \mathfrak{P}).$$

Das ist die Forderung a) in § 198.

Ist daher $\lambda_1, \lambda_2, \ldots, \lambda_n$ die Normalbasis in z, und $\mu_1, \mu_2, \ldots, \mu_n$ die komplementäre Basis, so ist:

$$(16)\quad \frac{dJ}{dz} = y_1\mu_1 + y_2\mu_2 + \cdots + y_n\mu_n,$$

worin die y_i ganze rationale Funktionen von z sind, woraus folgt, daß

$$(17)\quad S\left(\frac{dJ}{dz}\right) = y_1 \quad [\text{§ 198, (18)}]$$

eine ganze rationale Funktion von z ist.

Da diese Funktion hiernach keine negativen Potenzen von z enthalten kann, so ergibt sich aus (13) der zu beweisende Satz:

$$\overset{i}{\Sigma}\, a_{-1}^{(i)} = 0,$$

der mit der besonderen Annahme über die Variable z nichts mehr zu tun hat.

Als spezielle Anwendung folgt hieraus, daß ein Differential zweiter Gattung kein Residuum hat, und daß die beiden Residuen der Differentiale dritter Gattung gleich und entgegengesetzt sind.

Ein eigentliches Differential $d\sigma$, wie wir schon gesehen haben, hat kein Residuum, und die Residuen des „logarithmischen Differentials" $d\sigma : \sigma$ sind ganze Zahlen, nämlich die Ordnungszahlen in z.

Wir wollen diese Betrachtungen mit dem Beweis des folgenden Satzes beschließen:

> 4. Nennen wir Differentiale zweiter Gattung linear abhängig, wenn eine lineare Verbindung von ihnen und von Differentialen erster Gattung mit konstanten Koeffizienten einem eigentlichen Differential gleich ist, so sind höchstens $p + 1$ Differentiale zweiter Gattung immer linear abhängig.

Um dies zu beweisen, nehmen wir ein p-Eck zweiter Gattung:

$$(18) \qquad \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_p$$

mit p verschiedenen Punkten. Ist dann $\mathfrak{P}$ ein gegebener Punkt, so setzen wir:

$$(19) \qquad \mathfrak{U} = \mathfrak{P}\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_r$$

und erhalten eine Klasse B, in deren Teiler jedenfalls $\mathfrak{P}$ nicht aufgeht, weil sonst $\mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_n$ nach § 199, 7. von der ersten Gattung sein müßte. Wir können also eine Funktion in Ω:

$$(20) \qquad z = \frac{\mathfrak{A}}{\mathfrak{U}}$$

bestimmen, in deren Altereck jedenfalls der Punkt $\mathfrak{P}$ enthalten ist. Wir bilden nun das eigentliche Differential

$$(21) \qquad dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2},$$

in dessen Zähler $\mathfrak{Z}$ (dem Verzweigungspolygon nach z) der Punkt $\mathfrak{P}$ nicht aufgeht, weil er in $\mathfrak{U}$ nur einfach aufgeht, und wenn wir dz nach § 200, 4. durch Differentiale erster, zweiter und dritter

Gattung ausdrücken, so kann die dritte Gattung nicht in diesem Ausdruck vorkommen, weil sonst die Residuen nicht $= 0$ sein könnten. Dieser Ausdruck gibt also eine lineare Abhängigkeit zwischen den Differentialen zweiter Gattung, deren Unterecke $\mathfrak{P}^2, \mathfrak{P}_1^2, \mathfrak{P}_2^2, \ldots, \mathfrak{P}_p^2$ sind.

Nimmt man für irgend einen positiven Exponenten m:

$$\mathfrak{U} = \mathfrak{P}^{m-1} \mathfrak{P}_1 \mathfrak{P}_2 \ldots \mathfrak{P}_p,$$

und setzt

$$z = \frac{\mathfrak{A}}{\mathfrak{U}}, \quad dz = \frac{\mathfrak{Z}}{\mathfrak{U}^2},$$

so ist $\mathfrak{Z}$ durch $\mathfrak{P}^{m-2}$, $\mathfrak{U}^2$ durch $\mathfrak{P}^{2m-2}$, folglich das Untereck von dz durch $\mathfrak{P}^m$ teilbar. Man bekommt dann eine lineare Abhängigkeit zwischen den Differentialen mit den Unterecken

$$\mathfrak{P}^m, \mathfrak{P}^{m-1}, \ldots, \mathfrak{P}^2, \mathfrak{P}_1^2, \mathfrak{P}_2^2, \ldots, \mathfrak{P}_p^2,$$

und damit ist der Satz 4. allgemein bewiesen.

TABELLEN.

Tabelle I.

Entwickelungen der sechzehn ϑ-Quotienten (S. 88).

ν durchläuft alle ganzen Zahlen von $-\infty$ bis $+\infty$.

$$(1)\quad \frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{11}(a)} = 2i\sum\frac{e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}-1}.$$

$$(2)\quad \frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{10}(a)} = 2i\sum\frac{(-1)^{\nu}e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}-1}.$$

$$(3)\quad \frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{01}(a)} = 2i\sum\frac{q^{\nu}e^{\pi i v}\,e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}-1}.$$

$$(4)\quad \frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{00}(a)} = 2i\sum\frac{(-1)^{\nu}q^{\nu}e^{\pi i v}\,e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}-1}.$$

$$(5)\quad \frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{11}(a)} = -2i\sum\frac{e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}+1}.$$

$$(6)\quad \frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{10}(a)} = 2i\sum\frac{(-1)^{\nu}e^{2\pi i a\nu}}{q^{2\nu}e^{2\pi i v}+1}.$$

$$(7)\quad \frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{01}(a)} = 2\sum\frac{e^{2\pi i a\nu}q^{\nu}e^{\pi i v}}{q^{2\nu}e^{2\pi i v}+1}.$$

$$(8)\quad \frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{00}(a)} = 2\sum(-1)^{\nu}\frac{e^{2\pi i a\nu}q^{\nu}e^{\pi i v}}{q^{2\nu}e^{2\pi i v}+1}.$$

$$(9)\quad \frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\text{[illegible]}} = 2i\sum\frac{e^{(2\nu+1)\pi i a}}{q^{2\nu+1}e^{2\pi i v}-1}.$$

$$(10)\quad \frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{01}(v)\,\vartheta_{10}(a)} = -2\sum\frac{(-1)^{\nu}e^{(2\nu+1)\pi i a}}{q^{2\nu+1}e^{2\pi i v}-1}.$$

$$(11)\quad \frac{\vartheta_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{01}(v)\,\vartheta_{01}(a)} = 2i\sum\frac{e^{(2\nu+1)\pi i a}q^{\frac{2\nu+1}{2}}e^{\pi i v}}{q^{2\nu+1}e^{2\pi i v}-1}.$$

$$(12)\quad \frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{01}(v)\,\vartheta_{00}(a)} = -2\sum\frac{(-1)^{\nu}e^{(2\nu+1)\pi i a}q^{\frac{2\nu+1}{2}}e^{\pi i v}}{q^{2\nu+1}e^{2\pi i v}-1}.$$

(13) $$\frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{00}(v)\,\vartheta_{11}(a)} = -2i\sum\frac{e^{(2\nu+1)\pi i a}}{q^{2\nu+1}e^{2\pi i v}+1}.$$

(14) $$\frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{00}(v)\,\vartheta_{10}(a)} = 2\sum\frac{(-1)^{\nu}\,e^{(2\nu+1)\pi i a}}{q^{2\nu+1}e^{2\pi i v}+1}.$$

(15) $$\frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{00}(v)\,\vartheta_{01}(a)} = 2\sum\frac{e^{(2\nu+1)\pi i a}\,q^{\frac{2\nu+1}{2}}\,e^{\pi i v}}{q^{2\nu+1}e^{2\pi i v}+1}.$$

(16) $$\frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{00}(v)\,\vartheta_{00}(a)} = 2i\sum\frac{(-1)^{\nu}\,e^{(2\nu+1)\pi i a}\,q^{\frac{2\nu+1}{2}}\,e^{\pi i v}}{q^{2\nu+1}e^{2\pi i v}+1}.$$

Tabelle II.

Zweite Form der Entwickelung der sechzehn ϑ-Quotienten (S. 91).

In den Tabellen II, III, IV, V durchläuft m die Reihe der positiven geraden, n die Reihe der positiven ungeraden Zahlen, also:

$$m = 2, 4, 6, 8, 10, \ldots,$$
$$n = 1, 3, 5, 7, 9, \ \ldots$$

Ebenso soll m' die geraden, n' die ungeraden Zahlen durchlaufen.

(1) $$\frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{11}(a)} = \operatorname{cotg}\pi v + \operatorname{cotg}\pi a - 2i\sum\left[\frac{q^m e^{m\pi i a}}{e^{-2\pi i v} - q^m} - \frac{q^m e^{-m\pi i a}}{e^{2\pi i v} - q^m}\right].$$

(2) $$\frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{10}(a)} = \operatorname{cotg}\pi v - \operatorname{tg}\pi a - 2i\sum(-1)^{\frac{m}{2}}\left[\frac{q^m e^{m\pi i a}}{e^{-2\pi i v} - q^m} - \frac{q^m e^{-m\pi i a}}{e^{2\pi i v} - q^m}\right].$$

(3) $$\frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{01}(a)} = \frac{1}{\sin\pi v} + 2i\sum\left[\frac{q^{\frac{m}{2}} e^{-m\pi i a}\, e^{\pi i v}}{e^{2\pi i v} - q^m} - \frac{q^{\frac{m}{2}} e^{m\pi i a}\, e^{-\pi i v}}{e^{-2\pi i v} - q^m}\right].$$

(4) $$\frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{00}(a)} = \frac{1}{\sin\pi v} + 2i\sum(-1)^{\frac{m}{2}}\left[\frac{q^{\frac{m}{2}} e^{-m\pi i a}\, e^{\pi i v}}{e^{2\pi i v} - q^m} - \frac{q^{\frac{m}{2}} e^{m\pi i a}\, e^{-\pi i v}}{e^{-2\pi i v} - q^m}\right].$$

(5) $$\frac{\vartheta_{11}'\vartheta_{10}(v+a)}{\pi\vartheta_{10}(v)\vartheta_{11}(a)} = -\operatorname{tg}\pi v + \operatorname{cotg}\pi a - 2i\sum\left[\frac{q^m e^{-m\pi i a}}{e^{2\pi i v}+q^m} - \frac{q^m e^{m\pi i a}}{e^{-2\pi i v}+q^m}\right].$$

(6) $$\frac{\vartheta_{11}'\vartheta_{11}(v+a)}{\pi\vartheta_{10}(v)\vartheta_{10}(a)} = -\operatorname{tg}\pi v + \operatorname{tg}\pi a + 2i\sum(-1)^{\frac{m}{2}}\left[\frac{q^m e^{-m\pi i a}}{e^{2\pi i v}+q^m} - \frac{q^m e^{m\pi i a}}{e^{-2\pi i v}+q^m}\right].$$

(7) $$\frac{\vartheta_{11}'\vartheta_{00}(v+a)}{\pi\vartheta_{10}(v)\vartheta_{01}(a)} = \frac{1}{\cos\pi v} + 2\sum\left[\frac{q^{\frac{m}{2}} e^{m\pi i a} e^{\pi i v}}{q^m e^{2\pi i v}+1} + \frac{q^{\frac{m}{2}} e^{-m\pi i a} e^{-\pi i v}}{q^m e^{-2\pi i v}+1}\right].$$

(8) $$\frac{\vartheta_{11}'\vartheta_{01}(v+a)}{\pi\vartheta_{10}(v)\vartheta_{00}(a)} = \frac{1}{\cos\pi v} + 2\sum(-1)^{\frac{m}{2}}\left[\frac{q^{\frac{m}{2}} e^{m\pi i a} e^{\pi i v}}{q^m e^{2\pi i v}+1} + \frac{q^{\frac{m}{2}} e^{-m\pi i a} e^{-\pi i v}}{q^\pi e^{-2\pi i v}+1}\right].$$

(9) $$\frac{\vartheta_{11}'\vartheta_{01}(v+a)}{\pi\vartheta_{01}(v)\vartheta_{11}(a)} = \frac{1}{\sin\pi a} + 2i\sum\left[\frac{q^n e^{-n\pi i a}}{e^{2\pi i v}-q^n} - \frac{q^n e^{n\pi i a}}{e^{-2\pi i v}-q^n}\right].$$

(10) $$\frac{\vartheta_{11}'\vartheta_{00}(v+a)}{\pi\vartheta_{01}(v)\vartheta_{10}(a)} = \frac{1}{\cos\pi a} + 2\sum(-1)^{\frac{n-1}{2}}\left[\frac{q^n e^{-n\pi i a}}{e^{2\pi i v}-q^n} + \frac{q^n e^{n\pi i a}}{e^{-2\pi i v}-q^n}\right].$$

(11) $$\frac{\vartheta_{11}'\vartheta_{11}(v+a)}{\pi\vartheta_{01}(v)\vartheta_{01}(a)} = 2i\sum\left[\frac{q^{\frac{n}{2}} e^{-n\pi i a} e^{\pi i v}}{e^{2\pi i v}-q^n} - \frac{q^{\frac{n}{2}} e^{n\pi i a} e^{-\pi i v}}{e^{-2\pi i v}-q^n}\right].$$

(12) $$\frac{\vartheta_{11}'\vartheta_{10}(v+a)}{\pi\vartheta_{01}(v)\vartheta_{00}(a)} = 2\sum(-1)^{\frac{n-1}{2}}\left[\frac{q^{\frac{n}{2}} e^{-n\pi i a} e^{\pi i v}}{e^{2\pi i v}-q} + \frac{q^{\frac{n}{2}} e^{n\pi i a} e^{-\pi i v}}{e^{-2\pi i v}-q^n}\right].$$

$$(13) \quad \frac{\vartheta_{11}' \vartheta_{00}(v+a)}{\pi \vartheta_{00}(v) \vartheta_{11}(a)} = \frac{1}{\sin \pi a} + 2i \sum \left[\frac{q^n e^{n\pi i a}}{e^{-2\pi i v} + q^n} - \frac{q^n e^{-n\pi i a}}{e^{2\pi i v} + q^n} \right].$$

$$(14) \quad \frac{\vartheta_{11}' \vartheta_{01}(v+a)}{\pi \vartheta_{00}(v) \vartheta_{10}(a)} = \frac{1}{\cos \pi a} - 2 \sum (-1)^{\frac{n-1}{2}} \left[\frac{q^n e^{n\pi i a}}{e^{-2\pi i v} + q^n} + \frac{q^n e^{-n\pi i a}}{e^{2\pi i v} + q^n} \right].$$

$$(15) \quad \frac{\vartheta_{11}' \vartheta_{10}(v+a)}{\pi \vartheta_{00}(v) \vartheta_{01}(a)} = 2 \sum \left[\frac{q^{\frac{n}{2}} e^{n\pi i a} e^{-\pi i v}}{e^{-2\pi i v} + q^n} + \frac{q^{\frac{n}{2}} e^{-n\pi i a} e^{\pi i v}}{e^{2\pi i v} + q^n} \right].$$

$$(16) \quad \frac{\vartheta_{11}' \vartheta_{11}(v+a)}{\pi \vartheta_{00}(v) \vartheta_{00}(a)} = -2i \sum (-1)^{\frac{n-1}{2}} \left[\frac{q^{\frac{n}{2}} e^{n\pi i a} e^{-\pi i v}}{e^{-2\pi i v} + q^n} - \frac{q^{\frac{n}{2}} e^{-n\pi i a} e^{\pi i v}}{e^{2\pi i v} + q^n} \right].$$

Tabelle III.

Entwickelung der ϑ-Quotienten in trigonometrischen Reihen (S. 92).

(1) $$\frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{11}(a)} = \operatorname{cotg}\pi v + \operatorname{cotg}\pi a + 4\sum q^{\frac{m m'}{2}} \sin\pi(m a + m' v).$$

(2) $$\frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{10}(a)} = \operatorname{cotg}\pi v - \operatorname{tg}\pi a + 4\sum (-1)^{\frac{m}{2}} q^{\frac{m m'}{2}} \sin\pi(m a + m' v).$$

(3) $$\frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{01}(a)} = \frac{1}{\sin\pi v} + 4\sum q^{\frac{m n}{2}} \sin\pi(m a + n v).$$

(4) $$\frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{11}(v)\,\vartheta_{00}(a)} = \frac{1}{\sin\pi v} + 4\sum (-1)^{\frac{m}{2}} q^{\frac{m n}{2}} \sin\pi(m a + n v).$$

(5) $$\frac{\vartheta'_{11}\,\vartheta_{10}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{11}(a)}$$ Vertauschung von a und v in (2).

(6) $$\frac{\vartheta'_{11}\,\vartheta_{11}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{10}(a)} = \operatorname{tg}\pi v + \operatorname{tg}\pi a - 4\sum (-1)^{\frac{m+m'}{2}} q^{\frac{m m'}{2}} \sin\pi(m a + m' v).$$

(7) $$\frac{\vartheta'_{11}\,\vartheta_{00}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{01}(a)} = \frac{1}{\cos\pi v} + 4\sum (-1)^{\frac{n-2}{2}} q^{\frac{m n}{2}} \cos\pi(m a + n v).$$

(8) $$\frac{\vartheta'_{11}\,\vartheta_{01}(v+a)}{\pi\,\vartheta_{10}(v)\,\vartheta_{00}(a)} = \frac{1}{\cos\pi v} + 4\sum (-1)^{\frac{m+n-1}{2}} q^{\frac{m n}{2}} \cos\pi(m a + n v).$$